



**Atlantic Council**

GEOTECH CENTER



# **Report of the Commission on the Geopolitical Impacts of New Technologies and Data**





The Atlantic Council GeoTech Center works to shape the global future of data and technology together.

ISBN-13: 978-1-61977-178-9

This report is written and published in accordance with the Atlantic Council Policy on Intellectual Independence. The authors are solely responsible for its analysis and recommendations. The Atlantic Council and its donors do not determine, nor do they necessarily endorse or advocate for, any of this report's conclusions.

May 2021

**Cover:** Double Keck Lasers by Jason Chu Photography,  
<https://jason-chu.pixels.com>

**Website:** This report includes an interactive website,  
<https://atlanticcouncil.org/geotechreport>

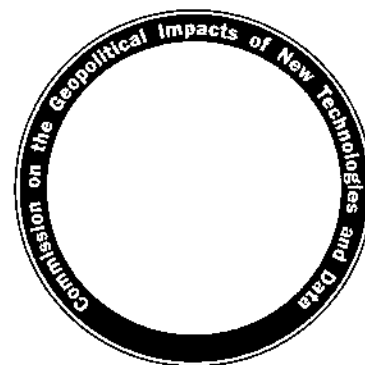
# Commission on the Geopolitical Impacts of New Technologies and Data

In preparing this report for the United States and its allies, to include members of Congress, the new presidential administration, private industry, academia, and like-minded nations, the Commission on the Geopolitical Impacts of New Technologies and Data sought to provide a compass bearing between where the world stood in 2020-2021 and a freer, more secure, and more prosperous world in 2031.

Data capabilities and new technologies impact geopolitics, global competition, and global opportunities for collaboration. The coming decade must address the sophisticated but potentially fragile systems that now connect people and nations, and incorporate resiliency as a necessary foundational pillar of modern life. To maintain national and economic security and competitiveness in the global economy, the United States and its allies must continue to be preeminent in key technology areas, and take measures to ensure the trustworthiness and sustainability of the digital economy, the analog economy, and their infrastructures to include:

- **Global science and technology leadership**
- **Secure data and communications**
- **Enhanced trust and confidence in the digital economy**
- **Assured supply chains and system resiliency**
- **Continuous global health protection and global wellness**
- **Assured space operations for public benefit**
- **Future of work**

The report's practical, implementable recommendations will enable the United States and like-minded nations to employ data capabilities and new technologies to achieve the goals set by this Commission.



#### Co-Chairs

Mr. John Goodman  
Ms. Teresa Carlson

#### Honorary Co-Chairs

Sen. Mark Warner  
Sen. Rob Portman  
Rep. Suzan DelBene  
Rep. Michael McCaul

#### Commissioners

Mr. Max R. Peterson II  
Mr. Paul Daugherty  
Mr. Maurice Sonnenberg  
Hon. Michael Chertoff  
Hon. Michael J. Rogers  
Mr. Pascal Marmier  
Ramayya Krishnan, PhD  
Hon. Shirley Ann Jackson, PhD  
Hon. Susan M. Gordon  
Vint Cerf, PhD  
Zia Khan, PhD  
Anthony Sciffignano, PhD  
Ms. Frances F. Townsend  
Admiral James Stavridis, USN, Ret.

#### Director & Executive Team

David A. Bray, PhD  
Peter Brooks, PhD  
Ms. Stephanie Wander

Mr. John Goodman, Co-Chair

Ms. Teresa Carlson, Co-Chair

David A. Bray, Director

# Executive Summary

---

**T**he advancing speed, scale, and sophistication of new technologies and data capabilities that aid or disrupt our interconnected world are unprecedented. While generations have relied consistently on technologies and tools to improve societies, we now are in an era where new technologies and data reshape societies and geopolitics in novel and even unanticipated ways. As a result, governments, industries, and other stakeholders must work together to remain economically competitive, sustain social welfare and public safety, protect human rights and democratic processes, and preserve global peace and stability.

Emerging technologies also promise new abilities to make our increasingly fragile global society more resilient. To sustain this progress, nations must invest in research, expand their digital infrastructures, and increase digital literacy so that their people can compete and flourish in this new era. Yet, at the same time, no nation or international organization is able to keep pace with the appropriate governance structures needed to grapple with the complex and destabilizing dynamics of these emerging technologies. Governments, especially democratic governments, must work to build and sustain the trust in the algorithms, infrastructures, and systems that could underpin society. The world must now start to understand how technology and data interact with society and how to implement solutions that address these challenges and grasp these opportunities. Maintaining both economic and national security and resiliency requires new ways to develop and deploy critical and emerging technologies, cultivate the needed human capital, build trust in the digital fabric with which our world will be woven, and establish norms for international cooperation.

The Commission on the Geopolitical Impacts of New Technologies and Data (GeoTech Commission) was established by the Atlantic Council in response to these challenges and seeks to develop recommendations to achieve these strategic goals. Specifically, the GeoTech Commission examined how the United States, along with other nations and global stakeholders, can maintain science and technology (S&T) leadership, ensure the trustworthiness and resiliency of physical and software/informational technology (IT) supply chains and infrastructures, and improve global health protection and wellness. The GeoTech Commission identified key recommendations and practical steps forward for the US Congress, the presidential administration, executive branch agencies, private industry, academia, and like-minded nations.



## The GeoTech Decade

Data capabilities and new technologies increasingly exacerbate social inequality and impact geopolitics, global competition, and global opportunities for collaboration. The coming decade—the “GeoTech Decade”—must address the sophisticated but potentially fragile systems that now connect people and nations, and incorporate resiliency as a necessary foundational pillar of modern life. Additionally, the rapidity of machines to make sense of large datasets and the speed of worldwide communications networks means that any event can escalate and cascade quickly across regions and borders—with the potential to further entrench economic inequities, widen disparities in access to adequate healthcare, as well as to hasten increased exploitation of the natural environment. The coming years also will present new avenues for criminals and terrorists to do harm; authoritarian nations to monitor, control, and oppress their people; and diplomatic disputes to escalate to armed conflict not just on land, sea, and in the air, but also in space and cyberspace.

### 2001-2011

**Decade of Counterterrorism**  
activities globally

### 2011-2021

**Decade of Decreasing Trust**  
in government and big  
technology companies

### 2021-2031

**GeoTech Decade** where  
technology and new data  
capabilities will significantly  
affect geopolitics, competition,  
and collaboration

Domestically and internationally, the United States must promote strategic initiatives that employ data and new technologies to amplify the ingenuity of people, diversity of talent, strength of democratic values, innovation of companies, and the reach of global partnerships.

## Geopolitical Impacts of New Technologies and Data Collections

Critical technologies that will shape the GeoTech Decade—and in which the United States and its allies must maintain global S&T leadership—can be grouped into six areas. All technologies in these categories will have broad—and interdependent—effects on people and the way they live and work, on global safety and security, and on the health of people and our planet.

- **Technologies that enable a digital economy: communications and networking, data science, and cloud computing:** collectively provide the foundation for secure transmission of data for both the public and private sector and establish robust economies of ideas, resources, and talent.
- **Technologies for intelligent systems: artificial intelligence, distributed sensors, edge computing, and the Internet of Things:** add new capabilities for

understanding changes in the world in both physical and digital environments. The resulting data may supplement human intelligence, social engagements, and other sources of insight and analysis. In select, defined areas, intelligent systems may enhance human governance of complex systems or decisions.

- **Technologies for global health and wellness: biotechnologies, precision medicine, and genomic technologies:** help create new fields of research, development, and practical solutions that promote healthy individuals and communities. Nations and health care organizations can use advances in genomics, or more broadly omics,<sup>1</sup> to provide sentinel surveillance<sup>2</sup> capabilities with respect to natural or weaponized pathogens. Sentinel surveillance can provide early detection, data about how a new element is appearing and growing, and information to guide our response.
- **Technologies that enlarge where people, enterprises, and governments operate: space technologies, undersea technologies:** commercial companies and nations around the world are deploying mega-constellations of satellites, or fleets of autonomous ocean platforms, with advanced, persistent surveillance and communications capabilities. Large-scale Earth observation data is important for monitoring the world's atmosphere, oceans, and climate as a foundation for understanding evolving health and environmental risks and increasing the economic efficiencies in transportation, agriculture, and supply chain robustness.
- **Technologies that augment human work: autonomous systems, robotics, and decentralized energy methods:** collectively provide the foundation to do work in dangerous or hazardous environments without risk to human lives, while at the same time augmenting human teams, potentially prompting long-term displacements in national workforces, and requiring additional workforce talent for new technology areas.
- **Foundational technologies: quantum information science (QIS), nanotechnology, new materials for extreme environments, and advanced microelectronics:** collectively provide the foundation for solving classes of computational problems, catalyzing next-generation manufacturing, setting standards, creating new ways to monitor the trustworthiness of digital and physical supply chains, as well

1 Omics technologies are primarily aimed at the universal detection of genes (genomics), mRNA (transcriptomics), proteins (proteomics), and metabolites (metabolomics) in a specific biological sample.

2 A sentinel surveillance system is used to obtain data about a particular disease that cannot be obtained through a passive system such as summarizing standard public health reports. Data collected in a well-designed sentinel system can be used to signal trends, identify outbreaks, and monitor disease burden, providing a rapid, economical alternative to other surveillance methods. Source: "Immunization Analysis and Insights," World Health Organization, accessed March 19, 2021, <https://www.who.int/teams/immunization-vaccines-and-biologicals/immunization-analysis-and-insights/surveillance/surveillance-for-vpds>.

as potentially presenting new challenges and opportunities to communications security that underpin effective governance and robust economies.

In addition to the technology itself, countries and organizations must learn to harness and protect the human element—by recruiting and upskilling workers with the needed skill sets for today and training the next generation with the right knowledge for tomorrow. There is great competition globally for digitally-skilled workers, and some countries or companies invest large amounts to develop or recruit this talent. When like-minded nations collaborate in S&T areas, the talent resources can produce greater benefits than possible otherwise. This requires governments to ensure their entire populations gain the needed digital literacy skills and have the means and opportunities to participate in the global digital economy. Making the whole greater than the sum of the parts represents the important global need for international collaboration.

The broad range of important S&T areas requires several forms of collaboration. In multiple key areas, such as QIS and advanced microelectronics, several nations already have significant government investments underway, and current results span a growing number of application areas. Collaborating on research and coordinating national investments among like-minded nations could benefit all participants. Fast-evolving technical capabilities, such as commercial space or autonomous systems, are supporting global industries that are developing and fielding new products. Effective collaboration relies on a broad ecosystem of domestic and foreign partners, including private sector entities. Collaboration will be limited in certain areas, for example, areas where, due to security considerations, the United States will develop capabilities in a self-reliant manner.

**Table ES.1: The GeoTech Decade: Areas Where Data and Technology Will Impact Social Equality, Geopolitics, Global Competition, and Global Opportunities for Collaboration**

### **Critical science and technology areas**

- Communications and networking, data science, cloud computing
- Artificial intelligence, distributed sensors, edge computing, the Internet of Things
- Biotechnologies, precision medicine, genomic technologies
- Space technologies, undersea technologies
- Autonomous systems, robotics, decentralized energy methods
- Quantum information science, nanotechnology, new materials for extreme environments, advanced microelectronics

## **Summary of Recommendations**

To maintain national and economic security and competitiveness in the global economy, the United States and its allies must

- Continue to be preeminent in key technology areas,
- Take measures to ensure the trustworthiness and sustainability of the digital economy, the analog economy, and their infrastructures.

The GeoTech Commission provides recommendations in the following six areas for achieving these strategic objectives. A seventh area, the Future of Work, discusses ways to ensure the workforce acquires the skills needed for the digital economy, and that there is equitable access to opportunity.

### **Global science and technology leadership**

To ensure that the United States and its allies remain the world leaders in S&T, the federal government, working with industry and stakeholders, should establish a set of prioritized strategic S&T objectives and align those objectives with specific timeframes. Additionally, the United States should establish a technology partnership among like-minded and democratic countries to coordinate actions around those objectives. The president and the US Congress should increase annual federal funding for research and development activities to secure US global leadership in critical new industries and technologies, with priorities determined for the largest impact challenges and gaps. To help people across the United States adapt to the realities of the future, the US government should establish programs to fund reskilling activities for workers displaced by changes brought about by the GeoTech Decade, seek new technologies and increase funding in support of efforts to close the broadband gap, and develop programs to improve the digital literacy of all Americans.

### **Secure data and communications**

To strengthen cybersecurity, the administration should update the implementation plan for the National Cyber Strategy. The strategy should streamline how public and private sector entities monitor the security of their digital environments; encourage new networking, computing, and software designs that strengthen cyber defense; and raise priorities and activities for the cybersecurity of operational technology—the hardware and software that keeps equipment running—to match those of information technology.

### **Enhanced trust and confidence in the global digital economy**

In order maintain the credibility of government and private industry, as well as to ensure prosperity, security, and stability in the coming data-driven epoch, the US government should establish new frameworks for data that incorporate security, accountability, auditability, transparency, and ethics. This means enacting measures that strengthen data privacy and security, establish transparency and ethics principles in how the government and private sector use data about people, and provide guidance on auditing how such data may be used.

### **Assured supply chains and system resiliency**

To ensure that the United States remains attuned to threats and weaknesses in supply chains and critical systems that power its future, the US government should develop a federal mechanism to assess and prioritize the importance of specific supply chains and systems to the nation, considering physical as well as software/IT supply chains and systems. The government should develop procedures and allocate resources to achieve sufficient resiliency, based on these priorities, for supply chains and critical systems to ensure the economic and national security of the United States.

### **Continuous global health protection and global wellness**

In order to protect the American people and environment from future threats, the US government should develop a global early warning system comprised of pandemic surveillance systems coupled with an early warning strategy, as well as a similar system aimed at providing early indicators of global environmental threats which could significantly impact the safety, security, and wellness of the nation.

### **Assured space operations for public benefit**

The US government should foster the growth of the commercial US space industrial base and leverage the increasing capabilities of large commercial satellite constellations. This could increase space mission assurance and deterrence by eliminating mission critical, single-node vulnerabilities and distributing space operations across hosts, orbits, spectrum, and geography.

**Table ES.2: Priority Recommendations**

<b>1. Global scientific and technology leadership</b>	1.1	Develop a National and Economic Security Technology Strategy
	1.2	Establish a Global GeoTech Alliance and Executive Council
	1.6	Establish national-scale training and education programs to foster continuing technological leadership
<b>2. Secure data and communications</b>	2A.1	Review, update, and reestablish the implementation plan for the National Cyber Strategy
	2A.2	Establish effective and coordinated continuous monitoring for software and hardware used by the federal government
	2A.4	Ensure cybersecurity best practices, expertise, and assurance testing are widely available to industry and government entities
	2B.1	Establish, with other nations, a common set of demonstration milestones for quantum data and communications security
	2B.3	Establish a program to accelerate the operationalization of quantum information science technologies
	2B.4	Establish leading roles for the United States in setting international standards for data and communications security as quantum information science evolves
<b>3. Enhanced trust and confidence in the global digital economy</b>	3.1	Develop a US data privacy standard
	3.4	Empower an organization to audit trust in the digital economy
	3.5	Assess standards relating to the trustworthiness of digital infrastructure
	3.6	Educate the public on trustworthy digital information
<b>4. Assured supply chains and system resiliency</b>	4.2	Fund and broaden federal oversight of supply chain assurance to include all critical resources
	4.3	For the United States, the administration must develop a geopolitical deterrence strategy that addresses critical digital resources and digital supply chain assurance
	4.4	Conduct regular physical and software/IT supply chain assessments in the United States and with allies, focused on intersecting vulnerabilities with cascading consequences
<b>5. Continuous global health protection and global wellness</b>	5.1	Develop a global early warning system comprised of pandemic surveillance systems coupled with an early warning strategy
	5.4	Increase resilience in medical supply chains
	5.5	Develop capacity building for vaccine and therapeutics discovery, development, and distribution
<b>6. Assured space operations for public benefit</b>	6.2	Foster commercial space technologies of strategic importance and protect these from foreign acquisition
	6.3	Harden the security of commercial space industry facilities and space assets
<b>7. Future of work</b>		Create the workforce for the GeoTech Decade, and equitable access to opportunity

Note: This table contains a subset of the full collection of recommendations.

Numbers refer to the recommendation sequence as discussed in the main chapters of the report.

# Table of Contents

Overview: Inflection Points	1
Table 1. Summary of the GeoTech Commission’s Findings and Recommendations	5
Table 2. List of All Recommendations of the Commission in Abridged Form	6
Chapter 1. Global Science and Technology Leadership	7
Chapter 2. Secure Data and Communications	17
Chapter 3. Enhanced Trust and Confidence in the Digital Economy	37
Chapter 4. Assured Supply Chains and System Resiliency	49
Chapter 5. Continuous Global Health Protection and Global Wellness	59
Chapter 6. Assured Space Operations for Public Benefit	69
Chapter 7. Future of Work	79
Conclusion	85
Appendix A. Additional Readings on Identifying and Countering Online Misinformation	88
Appendix B. Improving the Software Supply Chains and System Resiliency for the US Government	93
Appendix C. Advancing a Data Fabric for Achieving Continuous Global Health Protection	102
Appendix D. Additional Readings on the History and Future of Global Space Governance	107
Appendix E. Informational GeoTech Center Synopses	119
Appendix F. Additional Readings	128
Acronyms	129
Biographies of the GeoTech Commission Co-Chairs and Commissioners	134
Biographies of Supporting Atlantic Council Staff	145
Biographies of the Key Contributors to the GeoTech Commission Report	148
Acknowledgements	151

# Overview: Inflection Points

**A**ccelerating global connectedness—of people, supply chains, networks, economies, the environment, and other foundations of society—is changing how nations work together and compete. For example, the global spread of scientific and technology (S&T) knowledge has lessened the United States’ strategic advantage based on advanced technology. The global movement of people allows biological threats to spread worldwide, outpacing the world’s ability to respond. In the digital economy, the economic, governmental, and political parts of society are interconnected, with the potential for cybersecurity threats experienced in one context to reverberate in others.

This interconnectedness can lead to inflection points wherein current assumptions and practices are no longer valid or effective. Sources of strength or advantage can diminish. New vulnerabilities can be discovered, e.g., in global supply chains for hardware and software, and exploited. New approaches to protecting national interests in this globally connected world will rely, in many situations, on the cooperation and collaboration of like-minded nations to increase mutual knowledge and awareness. Without this focus, the detrimental aspects of globally connected systems and infrastructures will grow larger and become more urgent.

Each of the following areas is experiencing rapid change and each is critical for ensuring a secure and peaceful world. This overview discusses, for each chapter, the key issues, the opportunities and risks, and a characterization of what must be solved.

## **Chapter 1: Global Science and Technology Leadership**

The United States, with like-minded nations and partners, must collectively maintain continued leadership in key S&T areas to ensure national and economic security, and that technology is developed and deployed with democratic values and standards in mind. The United States must pursue, as strategic goals, establishing priorities, investments, standards, and rules for technology dissemination, developed across government, private industry, academia, and in collaboration with allies and partners. Collaboration among like-minded nations and partners is essential to the attainment of global S&T leadership.



## Chapter 2: Secure Data and Communications

Sophisticated attacks on the software/information technology (IT) supply chains have led to significant breaches in the security of government and private networks, requiring a new strategy for cybersecurity. This centers on updating and renewing the National Cyber Strategy Implementation Plan with a focus on streamlining how public and private sector entities monitor their digital environments and exchange information about current threats. Beyond these current challenges, advances in quantum information science (QIS) lay the foundation for future approaches to securing data and communications, to include new ways to monitor the trustworthiness of digital and physical supply chains. With allies and partners, the United States should develop priority global initiatives that employ transformative QIS.

## Chapter 3: Enhanced Trust and Confidence in the Global Digital Economy

Diminished trust and confidence in the global digital economy can constrain growth;<sup>3</sup> have destabilizing effects on society, governments, and markets; and lessen resilience against cascading effects of local, regional, or national economic, security, or health instabilities. Trust and confidence are diminished by practices that do not protect privacy or secure data, and by a lack of legal and organizational governance to advance and enforce accountability.<sup>4</sup> Automation and artificial intelligence (AI), essential for digital economies, pose challenges to how we organize and amplify the strength of both while minimizing their weakness or vulnerabilities in open societies. The United States should develop international standards and best practices for a trusted digital economy and should promote adherence to these standards.

## Chapter 4: Assured Supply Chains and System Resiliency

Both physical and digital supply chain vulnerabilities can have amplifying effects on the global economy and national security. To protect against these diverse risks requires understanding which types of goods and sectors of the economy are critical, and how to construct supply chains that are inherently more adaptable, resilient, and automated. This requires assessing the state and characteristics of supplies, trade networks and

3 Congressional Research Service, *Digital Trade and U.S. Trade Policy*, May 21, 2019, 11, accessed March 19, 2021, <https://crsreports.congress.gov/product/pdf/R/R44565>; in 2015, the Department of Commerce launched a Digital Economy Agenda, Alan B. Davidson, "The Commerce Department's Digital Economy Agenda," November 9, 2015, accessed March 19, 2021, <https://2014-2017.commerce.gov/news/blog/2015/11/commerce-departments-digital-economy-agenda.html>. This identifies four pillars: promoting a free and open Internet worldwide; promoting trust online; ensuring access for workers, families, and companies; and promoting innovation.

4 Philippe Amon, "Toward a New Economy of Trust" in *Revitalizing the Spirit of Bretton Woods: 50 Perspectives on the Future of the Global Economic System* (Washington, DC: Bretton Woods Committee), July 2019, accessed March 19, 2021, <https://www.brettonwoods.org/BW75/compendium-release>.

policies, inventory reserves, and the ability to substitute products or processing facilities. The United States should conduct regular assessments in the United States and in allied countries to determine critical supply chain resilience and trust, implement risk-based assurance measures, establish coordinated cybersecurity acquisition across government networks, and create more experts. A critical resource is semiconductor chip manufacturing, for which the vulnerability of foreign suppliers and the long lead time and cost of new production facilities requires the United States to invest in assured supply of semiconductor chips.

## Chapter 5: Continuous Global Health Protection and Global Wellness

Inherent to the disruption caused by the COVID-19 pandemic are three systemic problems: (i) global leaders acted slowly to contain the spread of the virus, (ii) global health organizations reacted slowly to contain the spread of the virus, and (iii) a mixture of factors caused the delayed response, including late recognition of the threat, slow incorporation of science and data into decision making, poor political will, and inconsistent messaging to citizens regarding the nature of the threat and what precautions to take. Though nations may adopt their own strategies to enhance resilience and future planning, a more global approach to this interconnected system will be essential. The United States and its allies should lead the effort to field and test new approaches that enable the world to accelerate the detection of biothreat agents, universalize treatment methods, and deploy mass remediation, through multiple global means. This is needed not only for recovering from the COVID-19 pandemic and future outbreaks, but also for human-developed pathogens.

## Chapter 6: Assured Space Operations for Public Benefit

The world is transforming from space assets being dominated almost entirely by government to being largely dominated by the private sector.<sup>5</sup> To maintain trusted, secure, and technically superior space operations, the United States must ensure it is a leading provider of needed space services and innovation in launch, on-board servicing, remote sensing, communications, and ground infrastructures. A robust commercial space industry not only enhances the resilience of the US national security space system by increasing space industrial base capacity, workforce, and responsiveness,

5 Simonetta Di Pippo, "Space Technology and the Implementation of the 2030 Agenda," *UN Chronicle* 55 (4) (January 2019): 61-63, accessed April 16, 2021, <https://www.un.org/en/chronicle/article/space-technology-and-implementation-2030-agenda>; Matt Weinzierl and Mehak Sarang, "The Commercial Space Age Is Here," *Harvard Business Review*, February 12, 2021, accessed April 16, 2021, <https://hbr.org/2021/02/the-commercial-space-age-is-here>; Matt Weinzierl, "Space, the Final Economic Frontier," *Journal of Economic Perspectives* 32 (2) (Spring 2018): 173-192, accessed April 16, 2021, [https://www.hbs.edu/ris/Publication%20Files/jep.32.2.173\\_Space,%20the%20Final%20Economic%20Frontier\\_413bf24d-42e6-4cea-8cc5-a0d2f6fc6a70.pdf](https://www.hbs.edu/ris/Publication%20Files/jep.32.2.173_Space,%20the%20Final%20Economic%20Frontier_413bf24d-42e6-4cea-8cc5-a0d2f6fc6a70.pdf); KPMG, *30 Voices on 2030: The future of space: Communal, commercial, contested*, May 2020, accessed April 16, 2021, <https://assets.kpmg/content/dam/kpmg/au/pdf/2020/30-voices-on-2030-future-of-space.pdf>.

but also advances a dynamic innovative environment that can bolster US competitiveness across existing industries, while facilitating the development of new ones. The United States should foster the development of commercial space technologies that can enhance national security space operations and improve agriculture, ocean exploration, and climate change activities, as well as align civilian and military operations and international treaties to support these uses.

## **Chapter 7: Future of Work**

People will power the GeoTech Decade, even as technology and data capabilities transform how people live, work, and operate as societies around the world. Successful societies will be those that found ways to augment human strengths with approaches to technology and data that were uplifting, while also working to minimize biases and other shortcomings of both humans and machines. Developing a digitally resilient workforce that can meet these challenges will require private and public sectors to take an all-of-the-above approach, embracing everything from traditional educational pathways to nontraditional avenues that include employer-led apprenticeships and mid-career upskilling. Ensuring that people are not left behind by the advance of technology—and that societies have the workforces they need to innovate and prosper—will determine whether the GeoTech Decade achieves its full promise of improving security and peace.

## **Appendices**

The remainder of the report includes the following appendices that discuss the technical foundations and potential solutions for several important challenges:

- Appendix A. Additional Readings on Identifying and Countering Online Misinformation
- Appendix B. Improving the Software Supply Chains and System Resiliency for the US Government
- Appendix C. Advancing a Data Fabric for Achieving Continuous Global Health Protection
- Appendix D. Additional Readings on the History and Future of Global Space Governance
- Appendix E. Informational GeoTech Center Synopses

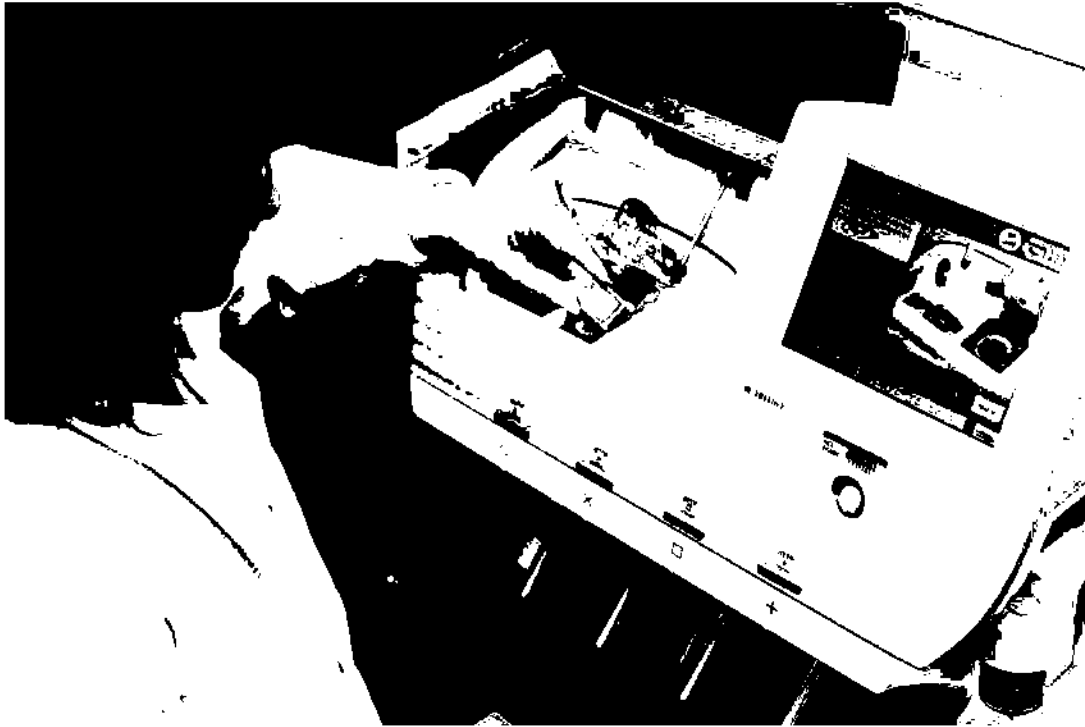
**Table 1. Summary of the GeoTech Commission's Findings and Recommendations**

	Findings	Recommendations
<b>1. Global science and technology leadership</b>	The US National Strategy for Critical and Emerging Technologies requires an implementation plan to guide both domestic and international coordination to achieve global science and technology leadership.	Establish priorities, investments, standards, and rules for technology dissemination; develop across government, private industry, academia, and with allies and partners.
<b>2. Secure data and communications</b>	Expanding cybersecurity vulnerabilities require partnerships between the public and private sectors.  Long-term quantum information science priorities include international collaboration, which is limited by national and regional funding and data sharing policies.	The United States should update and renew the National Cyber Strategy's Implementation Plan with a focus on streamlining how public and private sector entities monitor their digital environments.  With allies and partners, the United States should develop priority global initiatives that employ transformative quantum information science and catalyze the development of human capital and infrastructure for these and other next-generation quantum information science applications.
<b>3. Enhanced trust and confidence in the digital economy</b>	To enhance trust and confidence in artificial intelligence and other digital capabilities, technologies must objectively meet the public's needs for privacy, security, transparency, and accountability.	Develop international standards and best practices for a trusted digital economy that accommodate national rules and regulations, streamline the process of independently assessing adherence to these standards.
<b>4. Assured supply chains and system resiliency</b>	Resilient, trusted supply chains require defense, diversification, and reinvention.	Conduct regularized assessments in the United States and in allied countries to determine critical supply chain resilience and trust, implement risk-based assurance measures. Establish coordinated cybersecurity acquisition across government networks and create more experts.
<b>5. Continuous global health protection and global wellness</b>	There is a need for a continuous biological surveillance, detection, and prevention capability.	Field and test new approaches that enable the world to accelerate the detection of biothreat agents, to universalize treatment methods, and to engage in mass remediation, through multiple global means.
<b>6. Assured space operations for public benefit</b>	The US commercial space industry can increase its role in supporting national security.	Foster the development of commercial space technologies and develop a cross-agency strategy and approach to space that can enhance national security space operations and improve agriculture, ocean exploration, and climate change activities; align both civilian and military operations, and international treaties to support these uses.
<b>7. Future of Work</b>	Create the workforce for the GeoTech Decade, and equitable access to opportunity	

**Table 2. List of All Recommendations of the Commission in Abridged Form**

	Strategy	Governance & Leadership	Capabilities	International Allies
<b>1. Global science and technology leadership</b>	1.1 Develop National & Economic Security Technology Strategy	1.2 Establish Global GeoTech Alliance	1.4 Review nations' use of technology with focus on privacy, civil liberties, rights  1.5 Assess risks of technology applications ability to violate rights	1.3 Strengthen S&T collaboration  1.6 Establish training, education programs to foster technology leadership
<b>2. Secure data and communications</b>	2A.1 Strengthen National Cyber Strategy Implementation Plan  2B.2 Conduct QIS R&D focused on digital economy issues	2A.3 Bolster compliance with NIST guidance for continuous monitoring  2A.4 Ensure cybersecurity expertise, testing are widely available	2A.2 Coordinate gov't H/W, S/W monitoring  2B.3 Accelerate QIS technologies operationalization  2B.5 Establish national QIS infrastructure	2B.1 Establish shared quantum data and communications security milestones  2B.4 Set international data/communications standards
<b>3. Enhanced trust and confidence in the digital economy</b>	3.5 Assess digital infrastructure trustworthiness standards  3.6 Educate public on trustworthy digital information	3.1 Develop a US data privacy standard  3.4 Empower an organization to audit trust in the digital economy	3.3 Create measures and standards for digital economy trust  3.7 Demonstrate AI improvements to delivery of public- and private-sector services	3.2 Develop privacy-preserving technologies for the digital economy  3.8 Produce AI ethical, social, trust and governance assessment framework
<b>4. Assured supply chains and system resiliency</b>	4.3 Develop a geopolitical cyber deterrence strategy for critical digital resources	4.2 Broaden federal oversight of supply chain assurance	4.1 Identify and collect critical resource data	4.4 Assess physical and software/IT supply chain with allies
<b>5. Continuous global health protection and global wellness</b>	5.1 Launch a global pandemic surveillance and warning system	5.2 Reestablish extant pandemic monitoring  5.3 Prioritize privacy protections in pandemic surveillance	5.5 Develop vaccine, therapeutics capacity for discovery, development, distribution  5.6 Develop rapid responses to unknown pathogens	5.4 Increase medical supply chain resilience
<b>6. Assured space operations for public benefit</b>	6.1 Foster public benefits via federal space investments	6.3 Harden security of commercial space industry facilities and space assets	6.2 Foster and protect strategic space tech  6.5 Develop technologies for mega-constellation monitoring satellites	6.4 Establish conformance of commercial space systems to multinational agreements
<b>7. Future of work</b>	Create the Workforce for the GeoTech Decade, and Equitable Access to Opportunity			

# Chapter 1. Global Science and Technology Leadership



A lab technician loading a semiconductor DNA sequencing chip used to identify specific cancer mutations in an individual. A crucial component of science and technology leadership is rapidly training individuals and companies to employed advanced technology capabilities. Photo taken at the Advanced Technology Research Facility (ATRF) at the Frederick National Laboratory for Cancer Research, National Cancer Institute.

NATIONAL CANCER INSTITUTE VIA JUPITER

**T**he United States and like-minded nations, as well as private sector organizations, must continue to invest in and develop the multilateral mechanisms and academic and industrial capabilities, and the human capital needed for continued leadership in key science and technology (S&T) areas. Such leadership is essential for national and economic security and for ensuring that technology is developed and deployed with democratic values and standards in mind. The global development of advanced technologies requires the United States to pursue, as strategic goals and in collaboration with allies and partners, leadership in select areas.<sup>6</sup>

Six broad areas of S&T are critical to national and economic security, as follows:<sup>7</sup>

- 6 Democracy Technology Partnership Act, S. 604 — 117th Congress (2021-2022), 1st Session, accessed March 19, 2021, [https://www.warner.senate.gov/public/\\_cache/files/c/9/c9502023-85b4-4f7d-90db-9045237da704/18C2CE128388C4EC06C87EE8E4CEFB76.democracy-technology-partnership-act-bill-text.pdf](https://www.warner.senate.gov/public/_cache/files/c/9/c9502023-85b4-4f7d-90db-9045237da704/18C2CE128388C4EC06C87EE8E4CEFB76.democracy-technology-partnership-act-bill-text.pdf).
- 7 President's Council of Advisors on Science and Technology, *Recommendations for Strengthening American Leadership in Industries of the Future. A Report to the President of the United States of America*, June 2020, [https://science.osti.gov/-/media/\\_/pdf/about/pcast/202006/PCAST\\_June\\_2020\\_Report.pdf?la=en&hash=019A4F17C79FDEE5005C51D3D6CAC81FB31E3ABC](https://science.osti.gov/-/media/_/pdf/about/pcast/202006/PCAST_June_2020_Report.pdf?la=en&hash=019A4F17C79FDEE5005C51D3D6CAC81FB31E3ABC); White House, "National Strategy for Critical and Emerging Technologies," October 2020, accessed March 19, 2021, <https://sesecuritycenter.org/national-strategy-for-critical-and-emerging-technologies/>.

- **Communications and networking, data science, and cloud computing:** collectively provide the foundation for secure transmission of data for both the public and private sector and enable robust economies of ideas, resources, and talent. This critical area supports all aspects of a healthy digital economy domestically and internationally.
- **Artificial intelligence (AI), distributed sensors, edge computing, and the Internet of Things (IoT):** add new capabilities for understanding changes in the world for both physical and digital environments and enhance human governance in key, defined areas.
- **Biotechnologies, precision medicine, and genomic technologies:** collectively provide the foundation to heal and promote healthy individuals and communities, as well as to improve the performance of agricultural systems with regard to the reduction of atmospheric greenhouse gases, and to develop a system for early warning of emerging natural and human-produced risks such as outbreaks, bioterrorism, and environmental shocks.
- **Space technologies, undersea technologies, and new materials for extreme environments:** collectively provide for commercial companies and nations around the world to deploy mega-constellations of satellites, or fleets of autonomous ocean platforms, with advanced, persistent surveillance and communications capabilities to monitor the planet, including its oceans and environment, for emerging risks.<sup>8</sup>
- **Autonomous systems, robotics, and decentralized energy methods:** collectively provide the foundation to do work in dangerous or hazardous environments without risk to human lives, while at the same time augmenting human teams, potentially prompting long-term dislocations in national workforces, and requiring additional workforce talent for new technology areas.
- **Quantum information science (QIS), nanotechnology, and advanced micro-electronics:** collectively provide the foundation for solving classes of computational problems, next-generation manufacturing, new ways to monitor the trustworthiness of digital and physical supply chains, as well as potentially presenting new challenges to communications security that underpin effective governance and robust economies.

Participation by industry, academia, government labs, and US allies and partners will help ensure a fast pace of discovery and innovation. Achieving global S&T leadership also requires protecting intellectual property and proprietary information, and guiding

8 National Aeronautics and Space Administration, “Space Technology Grand Challenges,” December 2, 2010, accessed March 24, 2021, [https://www.nasa.gov/pdf/503466main\\_space\\_tech\\_grand\\_challenges\\_12\\_02\\_10.pdf](https://www.nasa.gov/pdf/503466main_space_tech_grand_challenges_12_02_10.pdf).

technology sharing with other nations based on their adherence to shared standards and values for security and privacy.

Technology sharing with non-allied nations poses strategic risks. For example, sharing advanced findings and applications of AI may benefit one nation at the expense of the other—AI-based image understanding algorithms could enhance remote sensing of military activities by commercial satellites. In other cases, new capabilities may benefit all nations, for example, a better disease testing technology.

**Finding 1: The US National Strategy for Critical and Emerging Technologies requires an implementation plan to guide both domestic and international coordination to achieve global science and technology leadership.**

The National Strategy for Critical and Emerging Technologies supports US national and economic security by promoting the National Security Innovation Base and by protecting the United States' technological advantage. Priority actions include developing the S&T workforce, establishing technology norms and standards that reflect democratic values and interests, ensuring research and development (R&D) funding of priorities, building strong partnerships with the private sector and with like-minded nations, and protecting the security of the technologies, their development, and how they are shared.<sup>9</sup> A detailed implementation plan, coordinated across the US government, is needed.<sup>10</sup>

**Finding 1.1: Achieving and sustaining technology leadership must be a long-term national priority.**

To achieve the long-term goals of technology leadership in key areas, a close and continuing interaction between S&T development and national security policy is essential.

The National Strategy for Critical and Emerging Technologies must be accompanied by long-term S&T goals resulting in demonstrations of significant import, and detailed programmatic plans for achieving these goals. The breadth of these technologies and their interdependencies require that progress should be shared with allies and partners and involve public-private partnerships (PPPs) among government research centers, private industry, and academia. This approach can catalyze human capital development and accelerate innovation.

9 White House, "National Strategy," 7-9.

10 US Government Accountability Office, *DoD Critical Technologies: Plans for Communicating, Assessing, and Overseeing Protection Efforts Should Be Completed*, GAO-21-158, January 2021, accessed April 16, 2021, <https://www.gao.gov/assets/gao-21-158.pdf>.



**Finding 1.2: Private sector research and development exceeds that of the government in some areas that are important for national and economic security, underscoring the need for greater coordination.**

The annual growth rate of domestic R&D government spending for 2000-2017 places the United States sixth, at 4.3 percent, behind the European Union (EU), Germany, India, South Korea, and China (17.3 percent).<sup>11</sup> The US government funds the largest share of basic research, while US industry funds the largest share of both applied research and development.<sup>12</sup>

Among the more important critical and emerging technologies are AI, quantum, cyber, digital infrastructure, and health/medical technologies, all areas in which private industry is growing. To strengthen US technology leadership, the United States must increase government R&D funding in critical areas and coordinate government and private industry R&D strategies.

**Finding 1.3: Recent proposed legislation addresses policies for guiding permissible technology development and use.**

Several countries are developing legislation to strengthen ethical practices underpinning data collection for AI algorithms, protect data privacy, and govern data rights.<sup>13</sup>

“Executive Order 13960 of December 3, 2020: Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government” establishes a set of principles governing the development and use of AI.<sup>14</sup>

A small sampling from recent, proposed US legislation includes the following ideas:

- Require assessments of the impacts of automated decision-making systems, including AI systems. These assessments would evaluate their accuracy, bias,

11 National Science Foundation, “The State of U.S. Science and Engineering 2020,” January 2020, accessed March 24, 2021, <https://ncses.nsf.gov/pubs/nsb20201/global-r-d>.

12 Congressional Research Service, “U.S. Research and Development Funding and Performance: Fact Sheet,” updated January 24, 2020, accessed March 26, 2021, <https://fas.org/sgp/crs/misc/R44307.pdf>; the National Academies defines federal S&T as essentially comprising funding categories 6.1 and 6.2. R&D is described as being more focused on application and development. Generally, government-funded S&T is dominated by academia and R&D is dominated by industry funding. For government-focused missions (e.g., NASA or DoD), the government funds industry directly for their R&D (either through contracts or independent R&D that is an allowable cost in contracts). This amount of R&D is still less than nongovernment industry R&D.

13 Law Library of the Library of Congress, *Regulation of Artificial Intelligence in Selected Jurisdictions*, January 2019, accessed March 26, 2021, <https://www.loc.gov/law/help/artificial-intelligence/regulation-artificial-intelligence.pdf>.

14 “Executive Order 13960 of December 3, 2020: Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government,” *Federal Register*, accessed March 26, 2021, <https://www.federalregister.gov/documents/2020/12/08/2020-27065/promoting-the-use-of-trustworthy-artificial-intelligence-in-the-federal-government>.

discrimination, privacy, and security.<sup>15</sup>

- Recommend approaches that promote the development and use of AI “while protecting civil liberties, civil rights, and economic and national security.”<sup>16</sup>
- Reinforce government regulations for protecting the privacy rights of individuals in terms of how data are collected, protected, used, and shared.
- Establish standards governing the responsible use of data and emerging technologies that include prohibitions on the use of personal data and emerging technologies in a manner that discriminates based on protected classes.

The European Commission established a High-Level Expert Group on Artificial Intelligence that published *Ethics Guidelines for Trustworthy AI* in April 2019. These guidelines address human agency and oversight, technical robustness and safety, privacy and data governance, transparency, diversity, nondiscrimination and fairness, societal and environmental well-being, and accountability.<sup>17</sup>

The newness of the technologies and their continuing evolution challenges the creation of internationally accepted, harmonized, and tested rules. In areas such as data privacy, harmonization of standards will require a heightening of US standards. In other areas of Internet and technology governance, the United States must have a leadership role in determining international standards and rules.

**Finding 1.4: Models for gaining technological leadership encourage innovation, focus on challenges concerning security or economic growth, organize governance, and draw from the global talent pool.**

A recent analysis, *Innovation Policies in the United States*,<sup>18</sup> discusses how these policies have changed over time, citing five models: “(i) Connected, challenge model, driven by societal challenges during World War II, where innovations are rapidly turned into capabilities, (ii) Basic science-focused, disconnected, decentralized model—the linear model during the Cold War, (iii) ‘Right-left’ translation model wherein the desired technologies motivate the basic science, (iv) Spanning the ‘valley of death’ model in which government initiatives helped bridge from basic research to the use of the innovations

15 Algorithmic Accountability Act of 2019, S. 1108 — 116th Congress (2019–2020), 1st Session, accessed March 26, 2021, <https://www.congress.gov/116/bills/s/1108/BILLS-116s1108is.pdf>.

16 AI in Government Act of 2020, H.R. 2575 — 116th Congress (2019–2020), accessed April 16, 2021, <https://www.congress.gov/bills/116th-congress/house-bill/2575/text>.

17 European Commission, “On Artificial Intelligence - A European approach to excellence and trust,” White Paper, Brussels, 19.2.2020, COM(2020) 65 final, accessed March 26, 2021, [https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020\\_en.pdf](https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf).

18 Bhavya Lal, “Innovation Policies in the United States,” Science and Technology Policy Institute, Institute for Defense Analyses, Washington, DC, accessed March 26, 2021, [https://gsdm.u-tokyo.ac.jp/file/170208\\_S2P2\\_Lal.pdf](https://gsdm.u-tokyo.ac.jp/file/170208_S2P2_Lal.pdf).

by industry, (v) Connected model in which societal needs connect innovation with the production of desired products.” The analysis concludes that “basic research must be complemented with additional institutional elements that reach much further down the innovation pipeline to development and later innovation stages.”

Proposed legislation introduced in the 116<sup>th</sup> Congress concerning AI research focused on convening “technical experts across academia, government, and industry to develop a detailed plan for how the United States can build, deploy, govern, and sustain a national AI research cloud.”<sup>19</sup> Another model for research collaboration was included in proposed legislation which would “organize a coordinated national strategy for developing AI, establish and support collaborative ventures or consortia with public or private sector entities, and accelerate the responsible delivery of AI applications from government agencies, academia, and the private sector.”<sup>20</sup> Both of these bills became law in Division E of the National Defense Authorization Act (NDAA): the Artificial Intelligence Initiative Act (Sections 5101-5105 of P.L.116-283) and the National AI Research Resource Task Force Act (Section 5106 of P.L.116-283).

The United States is a founding member of the Global Partnership on Artificial Intelligence (GPAI). “In collaboration with partners and international organizations, GPAI will bring together leading experts from industry, civil society, governments, and academia to collaborate across four Working Group themes: 1) Responsible AI; 2) Data Governance; 3) The Future of Work; and 4) Innovation & Commercialization,” according to a joint statement from the GPAI’s founding members.<sup>21</sup>

While the US model for funding R&D allows for multiple, independent lines of inquiry, in QIS, for example,<sup>22</sup> some coordination in international collaboration could help ensure a diversity of approaches is fostered.

19 US Sen. Rob Portman (R-OH), Portman, Heinrich Propose National Strategy For Artificial Intelligence; Call For \$2.2 Billion Investment In Education, Research & Development, press release, May 21, 2019, <https://www.portman.senate.gov/newsroom/press-releases/portman-heinrich-propose-national-strategy-artificial-intelligence-call-22>.

20 US Sens. Martin Heinrich (D-NM), Rob Portman (R-OH), and Brian Schatz (D-HI), in the 116th Congress sponsored the Artificial Intelligence Initiative Act (AI-IA), S. 1558, introduced in the Senate on May 21, 2019. Artificial Intelligence Initiative Act of 2019, S. 1558 — 116th Congress (2019-2020), <https://www.congress.gov/bills/116th-congress/senate-bill/1558>.

21 Department of State, “Joint Statement From Founding Members of the Global Partnership on Artificial Intelligence,” June 15, 2020, accessed March 26, 2021, <https://www.state.gov/joint-statement-from-founding-members-of-the-global-partnership-on-artificial-intelligence/>.

22 Subcommittee on Quantum Information Science under the Committee on Science of the National Science & Technology Council, *National Strategic Overview for Quantum Information Science*, September 2018, accessed March 26, 2021, [https://www.quantum.gov/wp-content/uploads/2020/10/2018\\_NSTC\\_National\\_Strategic\\_Overview\\_QIS.pdf](https://www.quantum.gov/wp-content/uploads/2020/10/2018_NSTC_National_Strategic_Overview_QIS.pdf).

**Approach 1: Focus the innovative work and talent on long-term capability demonstrations, while emphasizing democratic values.**

The United States and like-minded nations must be successful in each of the critical technology areas, or risk a vulnerability affecting national security. Success includes investing in innovative work and talent linked to long-term capability demonstrations. A focused approach sets concrete capability goals, constructs and funds fast-paced programs, and undergoes regular review. Talent from many nations and groups will make essential contributions. In contrast with nondemocratic nations, the United States and its allies and partners possess democratic values that can empower this work.

**Recommendation 1: Establish priorities, investments, standards, and rules for technology dissemination; develop across government, private industry, academia, and with allies and partners.**

**Recommendation 1.1: Develop a National and Economic Security Technology Strategy.**

To ensure the United States and its allies remain at the forefront of strategic S&T areas, the administration should develop a National and Economic Security Technology Strategy. The administration should create long-term S&T goals informed by assessments of foreign capabilities and plans. The National and Economic Security Technology Strategy should complement the National Security Strategy and draw upon the National Strategy for Critical and Emerging Technologies and other sources. The strategy should establish a long-term plan to direct government activities, incentivize private sector investments, enhance human capital, and develop capabilities in S&T that protect US national and economic security. The US Congress should conduct annual reviews of the milestone progress and budgets for these strategic S&T areas.

The strategy should also articulate a plan to establish a strategic technology ecosystem, including public-private partnerships, academia, industry, nonprofits, and others to accelerate technological development, support experimentation and pilot projects, and facilitate the application of new technologies to national and global challenges. Possible models include the Enduring Security Framework established by the National Security Agency (NSA), sector-specific consortia that include industry and academia, innovation labs that mature technology targeted at specific sectors, national laboratories developing large-scale test and evaluation infrastructure for advanced technology development, and focusing the National Science Foundation to address S&T.<sup>23</sup> The strategy should articulate ways to leverage not just the US workforce, but also the global talent base, while seeking to grow and retain existing highly skilled technical talent in the United States. The

23 Endless Frontier Act, H.R. 6978 / S. 3832 — 116th Congress (2019-2020), <https://www.aip.org/fyi/federal-science-bill-tracker/116th/endless-frontier-act>, introduced in the 116th Congress.

strategy should outline an approach that ensures the results of the strategic technology ecosystem provide the greatest public benefit possible from government investments.

The strategy should specifically address the following technology areas, with the strategic S&T goal for each area in italics:

1. Communications and networking, data science, and cloud computing: *provide the foundation for trustworthy digital infrastructures.*
2. Artificial intelligence (AI), distributed sensors, edge computing, and the Internet of Things (IoT): *testable, tunable, and trusted AI algorithms that are robust to limited, sparse, or corrupted data and require significantly less data, power, and time compared with today.*
3. Biotechnologies, precision medicine, and genomic technologies: *field a global system for fast, automated detection, diagnoses, and discovery of treatments for emerging pathogens, bioterrorism, and other environmental shocks to the planet.*
4. Space technologies, undersea technologies, and new materials for extreme environments: *monitor the entire planet pervasively and persistently, at high resolution and communicate the information in near-real time.*
5. Autonomous systems, robotics, and decentralized energy methods: *develop coordinated protocols for testing modular systems and methods and for evaluating emergent behaviors.*
6. Quantum information science (QIS), nanotechnology, and advanced microelectronics: *establish a national QIS infrastructure comprising research, development, computational, and testing programs, facilities, and skilled personnel; accelerate the operationalization of QIS technologies.*

#### **Recommendation 1.2: Establish a Global GeoTech Alliance and Executive Council.**

To ensure coordination between the US government and private sector on key S&T issues, the administration should create a Global GeoTech Alliance and Executive Council comprised of US private sector representatives and government representatives from the National Security Council, the Intelligence Community, the Department of Defense (DoD), the Department of State, the Treasury Department, the Department of Commerce, and the Office of the United States Trade Representative. This group—the Global GeoTech Alliance and Executive Council—would advise on issues arising from emerging technologies and data capabilities, technology cooperation, and technology standard-setting efforts, such as those raised in this report, and could provide the existing President's Intelligence Advisory Board with augmented membership and a honed focus on GeoTech issues of concern across sectors globally.

### **Recommendation 1.3: Strengthen international collaboration on science and technology.**

The administration should develop a strategy and a new multilateral mechanism among like-minded and democratic countries to coordinate technology policy, standards, and development. This strategy should seek to coordinate strategic S&T goals and milestones for collaborations with US allies and partner nations and develop agreements for sharing information, data, and research results. The strategy should also establish a framework for facilitating technical and programmatic information exchanges, with the goal of identifying opportunities for collaboration on specific S&T projects.

The administration should also increase participation by the United States in the GPAI.<sup>24</sup> The *William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021* directs the United States to establish several national AI programs and organizations to “ensure continued US leadership in artificial intelligence and to lead the world in the development and use of trustworthy artificial intelligence systems in the public and private sectors.”<sup>25</sup> This requires the United States to take a more active role in the GPAI—in GPAI leadership activities, AI strategy development multi-stakeholder experts group, and in the formulation and execution of the research agenda that supports the work of the multi-stakeholder experts group. Interfacing with the EU in support of the new seven-year Horizon Europe S&T initiative is another potential type of collaboration.

### **Recommendation 1.4: Conduct annual reviews on how nations use technology—with a focus on privacy, civil liberties, and human rights; use the findings to guide international cooperation.**

The administration should conduct an annual review that assesses the extent to which other nations use or develop S&T in ways that infringe upon the privacy, civil liberties, and human rights of their citizens, and undermine global peace and security. The results of the reviews should be used to help the United States prioritize cooperative efforts and facilitate coordination on S&T activities with other nations whose application of technology promotes peace, protects human rights, upholds the rule of law, and benefits global society. There is a recent proposal, for example, by the European Commission for a joint US-EU trade council.<sup>26</sup> This could be one of the focal points of this approach.

24 “The Global Partnership on Artificial Intelligence,” website homepage accessed on March 26, 2021, <https://www.gpai.ai/>.

25 William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, 117th Congress (2021-2022), Public Law No. 116-283, <https://www.congress.gov/bills/116th-congress/house-bill/6395>.

26 European Commission, EU-US: A new transatlantic agenda for global change, press release, December 2, 2020, Brussels, accessed March 26, 2021, [https://ec.europa.eu/commission/presscorner/detail/en/ip\\_20\\_2279](https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2279).

**Recommendation 1.5: Develop risk assessments of the ability of technology applications to violate civil rights, human rights, or undermine security.**

The administration should develop risk assessments<sup>27</sup> for technology applications to determine the potential of a technology application to violate human rights and civil liberties or to undermine security. The assessments also should identify ways to lessen the identified risks. The administration should develop an interagency process, involving the Department of Commerce, the DoD, the Department of State, the Office of the Director of National Intelligence, the Office of Science and Technology Policy, the National Institute of Standards and Technology, and the attorney general,<sup>28</sup> to carry out these risk assessments. The processes, criteria, and metrics should be open, transparent, and consistent with relevant US trade and export and import control laws.

**Recommendation 1.6: Establish national-scale training and education programs to foster continuing technological leadership.**

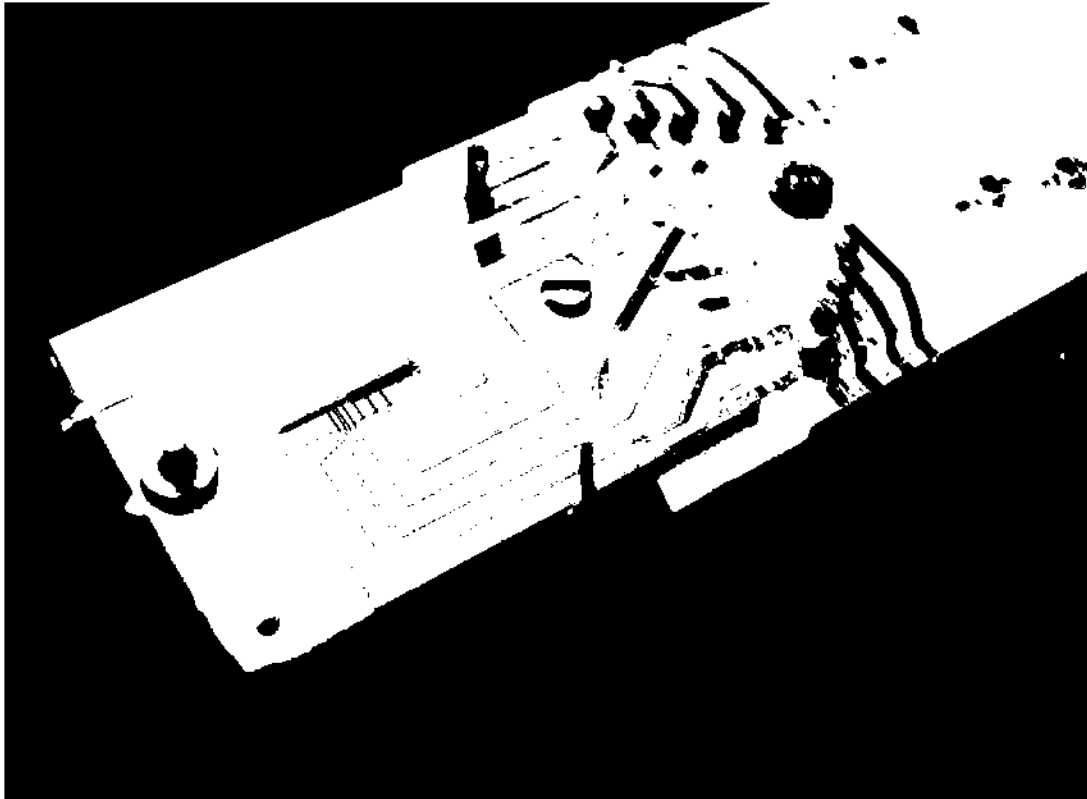
The administration should establish national-scale training and education programs to foster continuing technological leadership and to gain the strategic competitive advantage of being able to put advanced technologies to work quickly. The Department of Labor should establish a program that speeds up the matching of people to needed skills and rapidly trains individuals and companies in how to employ advanced technology capabilities. Current training methods cannot handle the fast-changing needs and numbers of students, and new mixtures of methods will evolve.<sup>29</sup> To help society participate in deciding how new technologies are developed and used, the administration should establish a national-scale educational program to inform the public about the benefits, risks, and brittleness of critical and emerging technologies.

27 Asena Baykal and Thorsten Benner, *Risky Business, Rethinking Research Cooperation and Exchange with Non-Democracies, Strategies for Foundations, Universities, Civil Society Organizations, and Think Tanks*, Global Public Policy Institute, October 2020, accessed March 26, 2021, [https://www.gppi.net/media/GPPI\\_Baykal\\_Benner\\_2020\\_Risky\\_Business\\_final.pdf](https://www.gppi.net/media/GPPI_Baykal_Benner_2020_Risky_Business_final.pdf).

28 Bureau of Industry and Security, "Scope of Export Administration Regulations, Part 734," Department of Commerce, accessed March 26, 2021, <https://www.bis.doc.gov/index.php/documents/regulations-docs/2382-part-734-scope-of-the-export-administration-regulations-1/file>.

29 Lee Rainie and Janna Anderson, "The Future of Jobs and Jobs Training," Pew Research Center, May 3, 2017, accessed March 26, 2021, <https://www.pewresearch.org/internet/2017/05/03/the-future-of-jobs-and-jobs-training/>.

# Chapter 2. Secure Data and Communications



NIST physicists demonstrated sustained, reliable quantum information processing in the ion trap at the left center of this photograph, improving prospects for building a practical quantum computer

PHOTOGRAPH BY  
NIST PHOTOGRAPHY  
PROGRAM  
PHOTOGRAPH BY  
ALBERTO CREMONA

**T**his chapter addresses secure data and communications in two timeframes. Part A discusses current cybersecurity concerns and includes recommendations for improving US cybersecurity against an expanding range of vulnerabilities. Part B focuses on quantum information science (QIS) and recommends steps for ensuring the United States, along with its allies and partners, remains a leader in the development and operationalization of QIS technologies.

## PART A: CURRENT CYBERSECURITY CONCERNS

Secure data and communications are fundamental to the United States' digital infrastructure and to attaining the full benefits of the global digital economy. Through the use of standards, risk assessments, monitoring, and technologies, the US government enables the public and private sectors to secure systems, data, and communications.

As the digital economy connects more public and private sector processes, effective cybersecurity for the US government faces several challenges: (i) the US government, through regulations, can affect though not assure the cybersecurity preparedness of



the private sector; (ii) the ultimate size of the needed cybersecurity workforce to secure US government and private sector networks requires the private sector to fulfill the larger share, though some small- and medium-sized companies cannot afford a dedicated cybersecurity workforce; and (iii) US government agencies and laws for ensuring cybersecurity are not fully adapted to the evolving characteristics of cyberattacks. The effects of these limitations will lead to more attack vectors, missed early warning indicators, and lower cybersecurity preparedness. To maintain secure data and communications, the United States must overcome these limitations and must also stay ahead of adversaries' exploitation of US network and endpoint vulnerabilities.

## **Finding 2A: Expanding cybersecurity vulnerabilities require partnerships between the public and private sectors.**

Cybersecurity vulnerabilities are increasing in scope and effect: greater connectivity yields more vectors for attacks, interdependent networks produce cascading effects, data breaches and records exposed are increasing,<sup>30</sup> and disjointed governance limits awareness and speed of action.

Cyberattackers leverage the interdependent parts of digital infrastructure to create complex attacks for the purposes of "coercion, sabotage, espionage, or extortion."<sup>31</sup> The greater number of connected devices can give attackers new, less defended points of access to systems and networks; for example, attackers could access the network controller devices in an electrical power network.<sup>32</sup> Software supply chains also present new cyberattack vulnerabilities when companies fail to employ industry-best security practices.

- In the recent SolarWinds Orion software supply chain attack, malware was inserted into a trusted software update, which led to significant breaches of government and private networks as the update was downloaded by as many as eighteen thousand SolarWinds customers (including other software and IT vendors). Such exploits of software/IT supply chains require knowledge of software configurations and dependencies. If a software vendor in the supply chain

30 Joseph Johnson, "Annual number of data breaches and exposed records in the United States from 2005 to 2020," Statista, March 3, 2021, accessed April 16, 2021, <https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/>; Joseph Johnson, "Number of data breaches in the United States from 2013 to 2019, by industry," Statista, March 9, 2021, <https://www.statista.com/statistics/273572/number-of-data-breaches-in-the-united-states-by-business/>.

31 U.S. Cyberspace Solarium Commission, *United States of America Cyberspace Solarium Commission Report*, March 2020, accessed March 26, 2021, <https://www.solarium.gov/report>.

32 Mission Support Center, "Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector: Mission Support Center Analysis Report," Idaho National Laboratory, August 2016, accessed March 26, 2021, <https://www.energy.gov/sites/prod/files/2017/01/f34/Cyber%20Threat%20and%20Vulnerability%20Analysis%20of%20the%20U.S.%20Electric%20Sector.pdf>.

is vulnerable, then its software updates become vectors for diffusing malware.<sup>33</sup>

Interdependencies among networks, including between digital infrastructures and physical systems or people, are a growing type of vulnerability. Three cases illustrate such interdependencies. In a cyber risk assessment of the election infrastructure, the Cybersecurity and Infrastructure Security Agency (CISA) found that “Disinformation campaigns conducted in concert with cyberattacks on election infrastructure can amplify disruptions of electoral processes and public distrust of election results.”<sup>34</sup> Ransomware attacks cost institutions money, caused inconvenience, and disrupted the healthcare at some hospitals.<sup>35</sup> An adversary could hold hostage one of the US critical infrastructure sectors<sup>36</sup> to preempt US military or diplomatic responses.

Data are as important as the networks, and are the foundation for new capabilities to monitor the climate, global health, agriculture, and cyberspace. Large data collections are essential for new applications of AI and innovations in medicine and education. The data infrastructure, including where the data are stored, analyzed, and the networks that communicate the results, are targets for cyberattacks.

Advanced cyberattacks take advantage of the limited information sharing between government cybersecurity experts and private industry, and the limited collection of cyberattack indicator information on private systems. Cyberattackers can spend weeks or months carefully probing the target systems, unnoticed.

Federal and private sector organizations lack sufficient insight into system operations, acquired software dependencies, and vendor practices. Also lacking is an effective system of liability and incentives to promote software supply chain security.

### **Finding 2A.1: Private sector infrastructure critical for economic or national security needs strengthened cybersecurity.**

Private sector enterprises and small businesses can be a vector for significant attacks on critical infrastructure, yet cannot readily access or benefit from US government

33 Ken Thompson, “Reflections on Trusting Trust,” *Communications of the ACM*, Volume 27 (8) (August 1984): 761-763, accessed March 26, 2021, [https://www.cs.cmu.edu/~rdriley/487/papers/Thompson\\_1984\\_ReflectionsonTrustingTrust.pdf](https://www.cs.cmu.edu/~rdriley/487/papers/Thompson_1984_ReflectionsonTrustingTrust.pdf).

34 Cybersecurity and Infrastructure Security Agency, “Election Infrastructure Cyber Risk Assessment,” Critical Infrastructure Security and Resilience Note, July 28, 2020, accessed March 26, 2021, [https://www.cisa.gov/sites/default/files/publications/cisa-election-infrastructure-cyber-risk-assessment\\_508.pdf](https://www.cisa.gov/sites/default/files/publications/cisa-election-infrastructure-cyber-risk-assessment_508.pdf).

35 Internet Crime Complaint Center, *Internet Crime Report 2020*, Federal Bureau of Investigation, accessed March 26, 2021, [https://www.ic3.gov/Media/PDF/AnnualReport/2020\\_IC3Report.pdf](https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf).

36 White House, President Barack Obama, “Presidential Policy Directive – Critical Infrastructure Security and Resilience, PPD-21,” February 12, 2013, accessed March 26, 2021, <https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil>.

cybersecurity expertise. According to *Securing Cyber Assets, Addressing Urgent Cyber Threats to Critical Infrastructure*:<sup>37</sup>

“[M]any outstanding federal capabilities play crucial roles in cyber defense and resilience today. However, their effectiveness is constrained in the following ways:

- Private sector knowledge of these [federal cybersecurity] capabilities and incentives to use them is limited.
- Access [to federal cybersecurity capabilities] is hindered by multiple legal and administrative constraints.
- Government capabilities are scattered across a wide swath of agencies, departments, and their sub-units—a complicated labyrinth comparatively few can effectively navigate.
- Classification of essential threat information can delay and hinder coordinated response.”

The following sources of cyber information and resources, along with improved coordination with the federal government, can address these needs: (i) Government sharing of critical information about cyberthreats, capabilities, and early attack indicators. This information can help private companies focus their cyberdefense resources and be more agile in doing so. (ii) A national cyber strategy that incorporates the private sector as an integral participant. This requires clarifying the laws governing the ability of the US government to direct the cybersecurity actions of private sector entities, including obligatory information sharing from certain private sector entities. (iii) For software/IT supply chains that support critical economic or national security infrastructure, US government provided risk information on vendors and components flowing into the software/IT supply chain, based on comprehensive and up-to-date collection of supply chain data and analysis of supply chain risks. Private industry can use this information to inform their risk assessments. (iv) US government incentives that assist private industry to grow the cybersecurity workforce needed to make the private sector more secure.

**Finding 2A.2: Obtaining the needed cybersecurity workforce and expertise requires participation by the public and the private sector.**

“Executive Order 13870 of May 2, 2019: America’s Cybersecurity Workforce,”<sup>38</sup> estab-

37 The President’s National Infrastructure Advisory Council, *Securing Cyber Assets: Addressing Urgent Cyber Threats to Critical Infrastructure*, August 2017, accessed March 26, 2021, <https://www.cisa.gov/sites/default/files/publications/niac-securing-cyber-assets-final-report-508.pdf>.

38 “Executive Order 13870 of May 2, 2019: America’s Cybersecurity Workforce,” *Federal Register*, accessed March 26, 2021, <https://www.federalregister.gov/documents/2019/05/09/2019-09750/americas-cybersecurity-workforce>.

lishes national requirements to expand both the federal cybersecurity workforce and the cybersecurity workforce for state, territorial, local, and tribal governments, academia, private sector stakeholders, and others. There are five hundred and twenty-one thousand unfilled cybersecurity jobs in the United States, of which thirty-seven thousand are in the federal government.<sup>39</sup>

The EO supports workforce mobility between the public and private sector for cybersecurity workers, and directs departments to share recruitment strategies and tools across these sectors. A starting point, for both sectors, is the Workforce Framework for Cybersecurity [National Initiative for Cybersecurity Education (NICE) Framework].<sup>40</sup> This defines categories and specialty areas, knowledge, tasks, skills, abilities, and work roles. It can be used by public and private sector employers to better match candidates with sets of needed skills.

To close the workforce gap in nonfederal positions, a flexible approach, consistent with the NICE Framework, may be effective.<sup>41</sup> The strategy is to develop new career models that are better matched to the pool of candidates, aligned with the NICE Framework where possible, and using employee development programs and financial incentives to grow workforce skills.

**Finding 2A.3: Cybersecurity governance, which must enable timely protective actions, has not matched the speed of the cyber threat environment.**

The National Institute of Standards and Technology (NIST) Cybersecurity Framework comprises five functions: Identify, Protect, Detect, Respond, and Recover.<sup>42</sup> In each function, timely action is essential for effective cybersecurity. Yet, defensive cybersecurity posture is systemically outpaced by offensive actors.

- Patching quickly is imperative. A FireEye study<sup>43</sup> reports the average time disclosure and patch availability was approximately nine days. Other

39 "Cybersecurity Supply/Demand Heat Map," Cyberseek.org, accessed March 26, 2021, <https://www.cyberseek.org/heatmap.html>.

40 National Initiative for Cybersecurity Careers and Studies, "Workforce Framework for Cybersecurity (NICE Framework)," Cybersecurity and Infrastructure Security Agency, accessed March 26, 2021, <https://niccs.cisa.gov/workforce-development/cyber-security-workforce-framework>.

41 Aspen Institute, *Principles for Growing and Sustaining the Nation's Cybersecurity Workforce*, November 2018, accessed March 26, 2021, <https://www.aspeninstitute.org/wp-content/uploads/2018/11/Aspen-Cybersecurity-Group-Principles-for-Growing-and-Sustaining-the-Nations-Cybersecurity-Workforce-1.pdf>.

42 "Cybersecurity Framework," National Institute of Standards and Technology, accessed March 26, 2021, <https://www.nist.gov/cyberframework/online-learning/five-functions>.

43 Kathleen Metrick, Jared Semrau, and Shambavi Sadayappan, "Think Fast: Time Between Disclosure, Patch Release and Vulnerability Exploitation — Intelligence for Vulnerability Management, Part Two," FireEye, April 13, 2020, accessed April 16, 2021, <https://www.fireeye.com/blog/threat-research/2020/04/time-between-disclosure-patch-release-and-vulnerability-exploitation.html>.

reports<sup>44</sup> have found longer times to patch though—up to thirty-eight days on average—and some of the most notorious cyber incidents exploited vulnerabilities patched months before their compromise.<sup>45</sup>

- Organizational adjustments and implementation of best practices must be rapid to keep up with developing threats. Yet, at the federal level, many agencies have been unable to adopt NIST-recommended best practices for ICT supply chain risk management for years.<sup>46</sup>
- Timely and rapid detection and response is necessary to forestall damage and the risk of cascading effects. This capability relies on a system of indicators and warnings, and, at times, comprehensive situational awareness that allows one to monitor cyber events closely and deploy defensive tools with precision. Still, the most sophisticated incursions can remain undetected for months.<sup>47</sup>
- Timely recovery depends on having built resilience into the digital infrastructure, and in having efficient decision making. Long-running attacks, however, can take more than a year to fully recover from.<sup>48</sup>
- All core cybersecurity functions depend on efficient information sharing between and within the public and private sectors. Yet, industry still complains about their incident response being hampered by liability concerns<sup>49</sup> and information sharing challenges.<sup>50</sup>

44 Rapid7, "Security Report for In-Production Web Applications," White Paper, accessed April 16, 2021, [https://www.rapid7.com/globalassets/\\_pdfs/whitepaperguide/rapid7-tcell-application-security-report.pdf](https://www.rapid7.com/globalassets/_pdfs/whitepaperguide/rapid7-tcell-application-security-report.pdf).

45 Amir Preminger, "NotPetya: Looking Back Three Years Later," Claroty, June 30, 2020, accessed April 16, 2021, <https://claroty.com/2020/06/30/notpetya-looking-back-three-years-later/>.

46 United States Government Accountability Office, *Information Technology: Federal Agencies Need to Take Urgent Action to Manage Supply Chain Risks*, GAO-21-171, December 15, 2020, accessed March 26, 2021, <https://www.gao.gov/assets/gao-21-171.pdf>.

47 Robert McMillan, "Hackers Lurked in SolarWinds Email System for at Least 9 Months, CEO Says," *Wall Street Journal*, February 2, 2021, accessed April 16, 2021, <https://www.wsj.com/articles/hackers-lurked-in-solarwinds-email-system-for-at-least-9-months-ceo-says-11612317963>.

48 Patrick Howell O'Neill, "Recovering from SolarWinds hack could take 18 months," *MIT Technology Review*, March 2, 2021, accessed April 16, 2021, <https://www.technologyreview.com/2021/03/02/1020166/solarwinds-brandon-wales-hack-recovery-18-months/>.

49 Cybersecurity and Infrastructure Security Agency, *Information and Communications Technology Supply Chain Risk Management Task Force Year 2 Report: Status Update on Activities and Objectives of the Task Force*, December 2020, accessed April 16, 2021, [https://www.cisa.gov/sites/default/files/publications/ict-scrim-task-force\\_year-two-report\\_508.pdf](https://www.cisa.gov/sites/default/files/publications/ict-scrim-task-force_year-two-report_508.pdf).

50 Lauren Feiner, "Microsoft president: The only reason we know about SolarWinds hack is because FireEye told us," *CNBC*, February 23, 2021, accessed April 16, 2021, <https://www.cnbc.com/2021/02/23/microsoft-exec-brad-smith-praises-fireeye-in-solarwinds-hack-testimony.html>.

**Approach 2A: Establish comprehensive situational awareness of cybersecurity risks in systems that are critical for national and economic security.**

The foundation of an effective cybersecurity strategy is comprehensive situational awareness of the state of the critical infrastructure for economic and national security. This is built upon the continuous collection of key indicators, prioritization of risk, the ability to assess key points in the software/IT supply chain, standards to inform best practices, and assessments of the actual levels of cyberdefense and resilience.

To achieve such comprehensive situational awareness requires that the public and private sectors must develop a partnership that ensures sufficient information is monitored and exchanged; that the authorities for taking action, when needed, are established in law; and that sufficient cybersecurity training and knowledge is available across the private sector to help strengthen the cybersecurity of this sector.

**Recommendation 2A: The United States should update and renew the National Cyber Strategy's Implementation Plan with a focus on streamlining how public and private sector entities monitor their digital environments.**

**Recommendation 2A.1: Review, update, and reestablish the Implementation Plan for the National Cyber Strategy.**

The administration should establish a process to incorporate both regular and ad hoc updates into the National Cyber Strategy so that the strategy remains current and evolves to meet future cybersecurity threats and challenges.<sup>51</sup> The strategy should retain focus on streamlining how public and private sector entities continuously monitor their digital environments to include outlining the appropriate roles, responsibilities, and governance. In addition to a single national cyber coordinator<sup>52</sup> that was established in the FY 2021 National Defense Authorization Act (NDAA), the strategy should consider the following components: uniform rules and increased compliance with standards for cybersecurity practices across all government activities (with exceptions for national security activities); skilled cybersecurity officers either in, or embedded in, organizations; and a national educational program to improve individuals' cybersecurity habits.

51 Government Accountability Office, *Cybersecurity: Clarity of Leadership Urgently Needed to Fully Implement the National Strategy*, report to congressional requestors, September 2020, accessed March 26, 2021, <https://www.gao.gov/assets/gao-20-629.pdf>; National Security Council, *National Cyber Strategy Implementation Plan* (Washington, D.C.: June 2019). The Implementation Plan was not published to the public, but any entity assigned a lead or supporting role within the plan received a digital copy of the plan.

52 William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021.

**Recommendation 2A.2: Establish effective and coordinated continuous monitoring for software and hardware used by the federal government.**

As part of COVID-19 pandemic relief, the America Rescue Plan Act of 2021 (Public Law No: 117-2, March 11, 2021)<sup>53</sup> includes \$1.65 billion for cybersecurity capabilities, readiness, and resilience. This increases the Technology Modernization Fund and helps CISA and the General Services Administration (GSA) complete modernization projects at federal agencies. Additional funds for CISA could bolster cybersecurity across federal civilian agency networks and support pilot programs for shared security and cloud computing services.

The acquisition strategies to achieve cybersecurity resilience should reflect the unique cybersecurity requirements and the need for specialized expertise in operations and networks supporting Title 5 (Government Organization and Employees), Title 10 (Armed Forces), Title 34 (Crime Control and Law Enforcement), and Title 50 (War and National Defense) of the US Code. The acquisition strategies should strengthen compliance with standards for continuous monitoring of cybersecurity performance.

The federal government should seek to achieve continuous cybersecurity monitoring of the hardware and software systems that support US government functions, including critical supply chains and network infrastructure. The approach should ensure coordination across all relevant elements of the federal government. Attributes to monitor include external network traffic, internal network behavior, vulnerability exposure, asset tracking, security posture, vendor compliance, product compliance, and product updates. There are four contributing activities to fully realize a cybersecurity posture informed by continuous monitoring: (i) assess the trustworthiness of software and hardware employed by the US government based on inherent vulnerabilities and risks due to the network position, permissions, and supply chain considerations; (ii) further empower the Department of Homeland Security (DHS) to perform these assessments by strengthening the ties among US government agency chief information officers (CIOs) and DHS for the various government networks; (iii) make these hardware and software risk assessments available to local and state governments to inform their endeavors; and (iv) leverage these assessments to support the private sector, especially small- to mid-sized businesses that do not have the capacity to fully assess their own supply chains yet would benefit from knowing what software is trustworthy. The risk assessments developed by the US government could also be shared with like-minded partners that are seeking to do the same regarding the hardware and software they employ to achieve assured supply chains and trusted digital environments.

There are several lines of effort, described further in Appendix B.

53 American Rescue Plan Act of 2021, H.R. 1319, Public Law No. 117-2, 117th Congress (2021-2022), <https://www.congress.gov/bills/117th-congress/house-bill/1319/text>.

**Recommendation 2A.3: Increase compliance with continuous monitoring that is part of the National Institute of Standards and Technology security control guidance.**

The administration should require GAO to review the efficacy of agency-specific practices regarding the continuous monitoring portion of its security control guidance. NIST controls dedicated to continuous monitoring for agencies<sup>54</sup> are required for all three priority levels of the federal agency information systems.<sup>55</sup> OMB memoranda as far back as 2011<sup>56</sup> discuss continuous monitoring superseding periodic reviews. While NIST has long recommended the practice, agencies have failed to implement it: in 2019, only about three-quarters had done so,<sup>57</sup> marking little improvement over several years. The most recent GAO report<sup>58</sup> indicates that general compliance with fundamental risk management practices has turned worse.

To achieve increased compliance, CISA should be empowered to assist lagging agencies in conforming with NIST guidelines and best practices mandated by the Federal Information Security Modernization Act (FISMA).<sup>59</sup> This would support a more responsive and uniform implementation of security methods—monitoring, security updates, approaches such as stress tests, assessing vendor security maturity, and certificate transparency. New data disclosure policies must be developed to enable the mapping, visualization, and testing of the software/IT supply chain networks.<sup>60</sup>

More specific understanding of the continuous monitoring practices is needed to guide implementation. There is overlap in the types of continuous monitoring discussed most often. First is the continuous monitoring of vendor compliance with certification regimes—the Federal Risk and Authorization Management Program (FedRAMP), the

54 “NIST Risk Management Framework,” National Institute of Standards and Technology Computer Security Resource Center, accessed March 26, 2021, <https://nvd.nist.gov/800-53/Rev4/control/CA-7>.

55 Kelley Dempsey et al., *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, Special Publication 800-137, NIST, September 2011, accessed March 26, 2021, <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-137.pdf>.

56 Office of Management and Budget, “FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management,” Executive Office of the President, Memorandum M-11-33, September 14, 2011, accessed March 26, 2021, <https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2011/m11-33.pdf>.

57 Executive Office of the President of the United States, *Federal Information Security Modernization Act of 2014: Annual Report to Congress, Fiscal Year 2019*, accessed March 26, 2021, <https://www.whitehouse.gov/wp-content/uploads/2020/05/2019-FISMARMAs.pdf>.

58 Government Accountability Office, *Information Technology: Federal Agencies Need to Take Urgent Action to Manage Supply Chain Risks*, GAO-21-171, December 15, 2020, accessed March 26, 2021, <https://www.gao.gov/products/GAO-21-171>.

59 *Federal Information Security Modernization Act of 2014*, S. 2521 — 113th Congress (2013-2014), <https://www.congress.gov/bill/113th-congress/senate-bill/2521/text>; FISMA requires each agency to handle its own security by meeting NIST SP 800-53 controls as well as requiring their information systems maintainers to comply with NIST SP 800-171. These NIST publications discuss continuous monitoring controls, with NIST SP 800-137 dedicated to even more, in depth consideration.

60 Cybersecurity and Infrastructure Security Agency, *Information and Communications Technology*.



Department of Defense (DoD) information networks approved product list (DoDIN APL), the new *Cybersecurity Maturity Model Certification (CMMC)*, etc. Each describes and aspires toward continuous assessment of compliance, but they are still organized around monthly, yearly, or three-year review periods. Truly continuous monitoring would bring more rigor and regularity to reviewing changes made to deployed software, a potentially devastating attack vector for adversaries, and changes in vendor security practices and context.

NIST guidelines refer to continuous monitoring of security control efficacy, asset exposure, threat vulnerability, configuration compliance, and other quasi-technical metrics. Between 79 percent and 83 percent of Chief Financial Officers Act of 1990 (CFO Act) federal agencies,<sup>61</sup> and between 58 percent and 63 percent of non-CFO Act agencies, fulfill these requirements. This type of continuous monitoring is determined by agency policy, leading to varying standards for how often to perform checks, what to check, and what satisfactory levels are.<sup>62</sup> A program at CISA, the Continuous Diagnostics and Mitigation (CDM) program, is supposed to integrate these activities. It has met systemic implementation difficulties, however,<sup>63</sup> and Homeland Security Secretary Alejandro Mayorkas has sought a review of the CDM program, along with CISA's EINSTEIN program, which monitors inbound and outbound traffic on federal networks.<sup>64</sup> It also must overcome great variation among the networks and products that would be checked. There is little agreement and the quality of implementation is not well-known.

Finally, there is the continuous monitoring of actual network behavior. This would include mandating the maintenance of standardized access logs, auditing of those logs, monitoring inbound and outbound traffic, and all the related detailed measurements. More transparency is needed in how much such monitoring occurs within government networks, though CISA's EINSTEIN program does the work of monitoring traffic in and out of federal civilian agencies.

**Recommendation 2A.4: Ensure cybersecurity best practices, expertise, and assurance testing are widely available to industry and government entities.**

The administration should provide the private sector technical information on threats on a regular basis, to bolster cybersecurity. The private sector outreach would be linked to the existing Information Sharing and Analysis Centers (ISACs) for US critical

61 Executive Office of the President of the United States, *Federal Information Security Modernization Act of 2014*.

62 Dempsey et al., *Information Security Continuous Monitoring (ISCM)*.

63 Congressional Research Service, *Cybersecurity: DHS and Selected Agencies Need to Address Shortcomings in Implementation of Network Monitoring Program*, August 2020, accessed March 26, 2021, <https://www.gao.gov/assets/gao-20-598.pdf>.

64 Justin Katz, "Mayorkas calls for review of Einstein, CDM," FCW, January 19, 2021, accessed March 26, 2021, <https://fcw.com/articles/2021/01/19/mayorkas-dhs-confirm-cyber.aspx>.

infrastructure entities and the Information Sharing and Analysis Organizations (ISAOs) to ensure monitoring of both supply chain risks and cybersecurity performance for vital US private sector companies of all sizes.

The US national security domain requires independent certification of adherence to a set of multinational standards.<sup>65</sup> One approach could be to expand CMMC to all of government instead of just DoD. While the program is still facing implementation challenges,<sup>66</sup> it could provide useful information on general cybersecurity maturity to industry and government alike, with benefits beyond the specific vendor products. Because DoD is only just beginning to implement CMMC, as a first step the administration should conduct a feasibility assessment for an across-government approach. To improve and streamline cybersecurity requirements, the administration should assess how a government-wide implementation of CMMC would overlap with FedRAMP or any other cybersecurity requirements, and how the broadened implementation of CMMC could improve general industry cyber hygiene.

To implement cybersecurity capabilities and practices, private sector companies must acquire cleared personnel, spaces, and IT equipment. The administration should consider accelerating any necessary prerequisite steps.

## PART B: QUANTUM INFORMATION SCIENCES

The United States, the European Union (EU), China, Russia, the United Kingdom, Canada, and other nations are expanding their investments in QIS, with national and regional QIS strategies and programs.<sup>67</sup> Recent demonstrations of quantum computers increase concerns that aspects of the technical foundation of the United States'

65 "Cybersecurity Maturity Model Certification (CMMC) Compliance," Compliance Forge, accessed March 26, 2021, <https://www.cmmc-compliance.com/>.

66 Jackson Barnett, "New bottleneck emerges in DOD's contractor cybersecurity program, concerning assessors," FEDSCOOP, April 19, 2021, accessed April 21, 2021, <https://www.fedscoop.com/cmmc-bottleneck-c3pao-assessments-dod/>.

67 Subcommittee on Quantum Information Science under the Committee on Science of the National Science & Technology Council, *National Strategic Overview*; "National Quantum Initiative Advisory Committee," US Department of Energy, accessed March 26, 2021, <https://science.osti.gov/About/NQIAC>; QUROPE Quantum Information Processing and Communication in Europe, *Quantum Technologies Roadmap*, European Union, August 2018, accessed March 26, 2021, <http://qurope.eu/h2020/qtflagship/roadmap2016>; National Development and Reform Commission, "The 13th Five Year Plan for Economic and Social Development of the People's Republic of China (2016-2020)," People's Republic of China, accessed March 26, 2021, [https://en.ndrc.gov.cn/newsrelease\\_8232/201612/P020191101481868235378.pdf](https://en.ndrc.gov.cn/newsrelease_8232/201612/P020191101481868235378.pdf); Arjun Kharpal, "In battle with U.S., China to focus on 7 'frontier' technologies from chips to brain-computer fusion," CNBC, March 5, 2021, accessed March 26, 2021, <https://www.cnbc.com/2021/03/05/china-to-focus-on-frontier-tech-from-chips-to-quantum-computing.html>.

digital security may be vulnerable in the foreseeable future.<sup>68</sup> Quantum communication and quantum key distribution (QKD) methods,<sup>69</sup> though, can enhance the security of the digital infrastructure. These methods may contribute to data and communications security against untrusted and corrupted hardware and also protect against the ability to make inferences about sensitive data based on access to multiple data sources containing nonsensitive data.<sup>70</sup>

**Finding 2B: Long-term quantum information science priorities include international collaboration, which is limited by national and regional funding and data-sharing policies.**

A primary element of leadership in QIS is the ability to set key standards for QIS applications. This relies on developing and deploying devices that operationalize QIS, and in working in collaboration with many nations and partners. While collaboration is identified as a national priority in the US national strategy for QIS, it should be extended beyond basic S&T activities.

**Finding 2B.1: The US strategy for quantum information science emphasizes US efforts and benefits.**

The *National Strategic Overview for Quantum Information Science*<sup>71</sup> provides a strategic approach for achieving US leadership in QIS and its applications to national and economic security. The six policy areas are as follows:

- **Choosing a science-first approach to QIS:** Strengthen the research foundation and the collaboration across disciplines. Use Grand Challenge problems as a strategic mechanism to coordinate and focus efforts.
- **Creating a future quantum-smart workforce:** Foster a QIS-skilled workforce through investments in industry, academia, and government laboratories that increase the scope of QIS research, development, and education.

68 S. Debnath et al., “Demonstration of a small programmable quantum computer with atomic qubits,” *Nature* 536 (2016): 63–66, accessed March 26, 2021, <https://doi.org/10.1038/nature18648>; Google AI Quantum and Collaborators et al., “Hartree-Fock on a superconducting qubit quantum computer,” *Science* 369 (6507) (August 28 2020): 1084–1089, accessed March 26, 2021, <https://doi.org/10.1126/science.abb9811>; Juan Yin et al., “Entanglement-based secure quantum cryptography over 1,120 kilometres,” *Nature* 582 (2020): 501–505, accessed March 26, 2021, <https://doi.org/10.1038/s41586-020-2401-y>; Vasileios Mavroedis et al., “The Impact of Quantum Computing on Present Cryptography,” *International Journal of Advanced Computer Science and Applications* 9 (3) (2018), accessed April 16, 2021, <https://arxiv.org/pdf/1804.00200.pdf>.

69 “Quantum Key Distribution (QKD) and Quantum Cryptography (QC),” National Security Agency Central Security Service, accessed March 26, 2021, <https://www.nsa.gov/what-we-do/cybersecurity/quantum-key-distribution-qkd-and-quantum-cryptography-qc/>.

70 M. Fujiwara et al. “Unbreakable distributed storage with quantum key distribution network and password-authenticated secret sharing,” *Scientific Reports* 6, 28988 (2016), accessed March 26, 2021, <https://doi.org/10.1038/srep28988>.

71 Subcommittee on Quantum Information Science under the Committee on Science of the National Science & Technology Council, *National Strategic Overview*.

- **Deepening engagement with the quantum industry:** Increase coordination among the federal government, industry, and academia to enhance awareness of needs, issues, and opportunities.
- **Providing critical infrastructure:** Encourage necessary investments, create and provide access to QIS infrastructure, and establish testbeds.
- **Maintaining national security and economic growth:** Maintain awareness of the security benefits and risks of QIS capabilities.
- **Advancing international cooperation:** Seek opportunities for international cooperation to benefit the US talent pool and raise awareness about other QIS developments.

The US strategy for QIS recognizes the sensitivities of this research, which can both enable new scientific and economic applications, and create new methods for attacking sensitive data and communications. This strategy supports international collaboration in QIS both to advance the basic research and its applications, and to ensure the United States maintains its leadership and competitiveness in QIS.<sup>72</sup>

- The US strategy for QIS supports international efforts in three ways: It reviews international research to maintain awareness of new results and directions, selects partnerships that will give the United States access to top-quality researchers and facilities, and shares certain public data from QIS research to help the development of standards for future QIS applications.

In addition to the US strategy for QIS, the National Quantum Initiative Act “authorized \$1.2 billion in federal research and development (R&D) spending over five years, established the National Quantum Coordination Office, and called for the creation of new QIS research institutes and consortia around the country.”<sup>73</sup> Also, the National Science Foundation (NSF) recently established three quantum research centers<sup>74</sup> and added the opportunity for limited supplemental funding requests to support international collaboration on basic research topics.<sup>75</sup>

<sup>72</sup> Ibid.

<sup>73</sup> National Quantum Initiative Act of 2018. S. 3143, Public Law No. 115-368, 115th Congress (2017-2018), accessed March 26, 2021, <https://www.congress.gov/115/plaws/publ368/PLAW-115publ368.pdf>.

<sup>74</sup> National Science Foundation, “NSF establishes 3 new institutes to address critical challenges in quantum information science,” Announcement, July 21, 2020, accessed March 26, 2021, [https://www.nsf.gov/news/special\\_reports/announcements/072120.jsp](https://www.nsf.gov/news/special_reports/announcements/072120.jsp).

<sup>75</sup> “Dear Colleague Letter: International Collaboration Supplements in Quantum Information Science and Engineering Research,” National Science Foundation, NSF 20-063, March 24, 2020, accessed March 26, 2021, <https://nsf.gov/pubs/2020/nsf20063/nsf20063.jsp>.

Congressional hearings on “Industries of the Future” discussed the importance of QIS and establishing US leadership in QIS.<sup>76</sup> One effort by the United States to establish international cooperation in QIS is the agreement between the United States and Japan to cooperate on quantum research through activities including “collaborating in venues such as workshops, seminars, and conferences to discuss and recognize the progress of research in QIST, which in turn will lead to the identification of overlapping interests and opportunities for future scientific cooperation.”<sup>77</sup>

**Finding 2B.2: China is pursuing quantum information science as a strategic technology.**

Quantum communications and computing are among the strategic technologies highlighted in China’s 14<sup>th</sup> Five-Year Plan (2021-2025). China aims to be a global leader in innovation, using large demonstration projects to advance its science and technology (S&T), and to build human capital for strategic technology areas. This includes major initiatives in quantum research and development (R&D), demonstrations of QKD and quantum computing, and a major new National Laboratory for Quantum Information Sciences.<sup>78</sup> China is able to advance in quantum R&D in part due to the close coordination among the government, universities, and industry, which aids both the advancement of the science and the building of a skilled workforce.<sup>79</sup>

**Finding 2B.3: EU’s science and technology strategy focuses on EU participation.**

The EU’s S&T program includes three components that address QIS and other technology areas: (i) Horizon Europe, which has a seven-year budget of €95.5 billion for 2021-2027, within which the Digital, Industry and Space area is funded at €15.5 billion;<sup>80</sup> (ii)

76 “Industries of the Future,” U.S. Senate Committee on Commerce, Science, and Transportation, January 15, 2020, accessed March 26, 2021, <https://www.commerce.senate.gov/2020/1/industries-of-the-future>.

77 “Tokyo Statement on Quantum Cooperation,” U.S. Department of State, December 19, 2019, accessed March 26, 2021, <https://www.state.gov/tokyo-statement-on-quantum-cooperation/>.

78 Elsa B. Kania, “China’s Quantum Future,” *Foreign Affairs*, September 26, 2018, <https://www.foreignaffairs.com/articles/china/2018-09-26/chinas-quantum-future>; European Commission, “Quantum Technologies Flagship kicks off with first 20 projects,” Factsheet, October 29, 2018, accessed March 26, 2016, [https://ec.europa.eu/commission/presscorner/detail/de/MEMO\\_18\\_6241](https://ec.europa.eu/commission/presscorner/detail/de/MEMO_18_6241); Arjun Kharpal, “In battle with U.S., China to focus on 7 ‘frontier’ technologies from chips to brain-computer fusion,” *CNBC*, March 5, 2021, accessed March 26, 2021, <https://www.cnbc.com/2021/03/05/china-to-focus-on-frontier-tech-from-chips-to-quantum-computing.html>; Lauren Dudley, “China’s Quest for Self-Reliance in the Fourteenth Five-Year Plan,” *Net Politics*, March 8, 2021, accessed April 16, 2021, <https://www.cfr.org/blog/chinas-quest-self-reliance-fourteenth-five-year-plan>.

79 Martin Giles, “The man turning China into a quantum superpower,” *MIT Technology Review*, December 19, 2018, accessed March 26, 2021, <https://www.technologyreview.com/2018/12/19/1571/the-man-turning-china-into-a-quantum-superpower/>.

80 “Final budget breakdown Horizon Europe,” Science&Business, accessed April 16, 2021, [https://sciencebusiness.net/sites/default/files/inline-files/Final%20budget%20breakdown%20Horizon%20Europe\\_0.pdf](https://sciencebusiness.net/sites/default/files/inline-files/Final%20budget%20breakdown%20Horizon%20Europe_0.pdf).

Digital Europe Programme, funded at €7.5 billion;<sup>81</sup> and (iii) Space Programme, with proposed funding of €13.2 billion.<sup>82</sup> The European Commission is soliciting proposals for quantum communications infrastructure, which will be funded by these initiatives. The objective is to enable the EU to be an independent provider of quantum technologies needed to build a quantum communications infrastructure.<sup>83</sup>

Horizon 2020, the predecessor to Horizon Europe, involved US researchers in only 1.5 percent of the Horizon 2020 projects.<sup>84</sup> In comparison, EU researchers participate at a much greater level considering all National Science Foundation (NSF) and National Institutes of Health (NIH) active grants.<sup>85</sup> This asymmetry in participation is due to EU rules that require participants in Horizon 2020 projects to sign grant agreements. For US institutions, this raises issues concerning “governing law and jurisdiction, intellectual property treatment, joint and several liability<sup>86</sup> and indemnification, access to data and implications for export control, and auditing requirements.”<sup>87</sup>

#### **Finding 2B.4: Funding policies constrain collaboration.**

One issue of concern in the Horizon Europe initiative rules governing participation is the determination of financial contribution by the United States and “third countries” as defined in Article 12 of Horizon Europe—the Framework Programme for Research

81 “Digital Europe Programme,” European Commission, accessed April 16, 2021, <https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/programmes/digital>.

82 European Commission, Commission welcomes the political agreement on the European Space Programme, press release, December 16, 2020, accessed April 16, 2021, [https://ec.europa.eu/commission/presscorner/detail/en/IP\\_20\\_2449](https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2449).

83 European Commission, “European Commission, Call for tenders CNECT/LUX/2020/CPN/0062, Detailed system study for a Quantum Communication Infrastructure, Competitive Procedure with Negotiation,” accessed April 16, 2021, [https://ec.europa.eu/newsroom/dae/document.cfm?doc\\_id=69304](https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=69304); Éanna Kelly, “Switzerland pencilled back into quantum plans, but no access for UK, Israel,” Science|Business, March 18, 2021, accessed April 16, 2021, <https://sciencebusiness.net/news/switzerland-pencilled-back-quantum-plans-no-access-uk-israel>; “Horizon Europe, Work Programme 2021-2022, 7. Digital, Industry and Space,” European Commission, accessed April 16, 2021, <https://sciencebusiness.net/sites/default/files/inline-files/7.%20Digital%20Industry%20Space.pdf>.

84 CORDIS, European Commission Research Results, accessed April 16, 2021, <https://cordis.europa.eu/projects/en>. This represents a comparison of Horizon 2020 projects originating in the United States during 2013-2020 with the total number of Horizon 2020 projects, excluding certain subcategories from both groupings.

85 “Funding & tender opportunities, Single Electronic Data Interchange Area (SEDIA),” European Commission, accessed March 26, 2021, <https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/horizon-dashboard>.

86 “When two or more parties are jointly and severally liable for a tortious act, each party is independently liable for the full extent of the injuries stemming from the tortious act.” “Joint and Several Liability,” Cornell Law School, accessed March 26, 2021, [https://www.law.cornell.edu/wex/joint\\_and\\_several\\_liability](https://www.law.cornell.edu/wex/joint_and_several_liability).

87 Richard L. Hudson, “Tale of two cities: Brussels and Washington struggle to cooperate in science,” Science|Business, May 14, 2018, accessed April 16, 2021, <https://sciencebusiness.net/tale-two-cities-brussels-and-washington-struggle-cooperate-science>; Ryan Lankton and Jennifer Ponting, “Managing Horizon 2020 Grants: the Experiences of the University of Michigan and Harvard,” *NCURA Magazine*, National Council of University Research Administrators, XLVIII (1) (January/February 2016), accessed April 16, 2016, <http://www.ncura.edu/portals/0/docs/srag/january%202016%20issue-weibo.pdf>.

and Innovation.<sup>88</sup> The calculated cost of association with the Horizon Europe initiative is based on the relative size of a country's gross domestic product (GDP) compared with EU GDP. For example, the European Commission has proposed making the UK pay a proportion of the 2021-2027 research budget based on its share of EU GDP, which currently stands at 18 percent. For the United States, this corresponding value is 137 percent, yielding a required contribution of \$131.4 billion.

The regulations establishing Horizon Europe contain other potential issues for US participation. These include Article 36, which gives the European Commission rights regarding transfer and licensing, and Article 49, which gives certain EU entities the right to carry out investigations and inspections.

**Approach 2B: Coordinate with allies and partners to build human capital for quantum information science and overcome limitations imposed by national and regional funding and data-sharing policies.**

In the ongoing competitive R&D of QIS, key determinants of success are the size, skill, and collaboration of the technology workforce spanning a number of disciplines, including those in the fields of science, technology, engineering, mathematics (STEM), and manufacturing. The United States recognizes that it "must work with international partners, even while advancing domestic investments and research strategies."<sup>89</sup>

**Recommendation 2B: With allies and partners, the United States should develop priority global initiatives that employ transformative quantum information science and catalyze the development of human capital and infrastructure for these and other next-generation quantum information science applications.**

**Recommendation 2B.1: Establish, with other nations, a common set of demonstration milestones for quantum data and communications security.**

The administration should extend the technological development portfolio of national investments in QIS to incorporate a common set of milestones with allies. The members of the National Science and Technology Council (NSTC) Subcommittee on Quantum Information Science should develop such milestones in coordination with representatives from collaborating nations. These are to be consonant with plans by the United States and like-minded nations to develop testbeds, demonstrations, standards, and a quantum-skilled workforce. The milestones will inform the practical applications for use

88 "Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL establishing Horizon Europe - the Framework Programme for Research and Innovation, laying down its rules for participation and dissemination - Common understanding," Council of the European Union, Interinstitutional File: 2018/0224(COD), accessed March 26, 2021, <https://www.consilium.europa.eu/media/38902/st07942-en19.pdf>.

89 Subcommittee on Quantum Information Science under the Committee on Science of the National Science & Technology Council, *National Strategic Overview*, 12.

with near-, mid-, and long-term levels of quantum information capabilities. The EU's Horizon Europe initiative is a potential opportunity for such collaboration. The United States should also establish data sharing agreements with other nations for QIS results pertaining to shared economic and national security interests.

**Recommendation 2B.2: Create a program of quantum information science research and development focused on emerging issues for digital economies.**

The administration should continuously evaluate QIS progress and technologies through the White House Office of Science and Technology Policy (OSTP) and the National Academies of Sciences, Engineering, and Medicine; this could be accomplished by the creation of a standing committee such as they have done for other areas that will be long-lived. This will identify new technology directions, review QIS policies, and revisit priorities and partnerships. The evaluations should focus on entirely new quantum capabilities that can benefit digital economies, e.g., privacy and advances in biotechnology and data capabilities, open sharing of data while maintaining data privacy, principles for systems to be quantum-secure by design, digital supply chain security for both hardware and software, evolution of Internet protocols, network modernization, and other topics.

**Recommendation 2B.3: Establish a program to accelerate the operationalization of quantum information science technologies.**

Recognizing the need for broad and significant investment in quantum applications to focus and accelerate progress, Congress and the administration should establish a program, led by the Defense Advanced Research Projects Agency (DARPA), to accelerate the operationalization of continually evolving hybrid (classical and quantum) computing architectures. This program will mature prototype demonstrations of quantum computing, communication, sensing, and metrology technologies to yield fieldable capabilities. The program also should include elements that seek to develop a quantum-skilled workforce in the private and public sectors. Several models for such a program are seen in DARPA's long history of rapidly growing and maturing advanced technology fields, e.g., Grand Challenges for autonomous vehicles, Have Blue for stealth technologies, and AI Next for artificial intelligence.

**Recommendation 2B.4: Establish leading roles for the United States in setting international standards for data and communications security as quantum information science evolves.**

Building on the results obtained from NDAA FY 2021, SEC. 9414, *Study on Chinese Policies and Influence in the Development of International Standards for Emerging*



*Technologies*,<sup>90</sup> the administration should take steps to bolster the development of standards for QIS technology development and applications.<sup>91</sup> This will drive toward a strategy for achieving a leadership role in international quantum standards setting, sharing sensitive security-related advances with allies, responding to China's efforts to influence international standards,<sup>92</sup> and catalyzing private sector investments in quantum technologies. NIST is currently developing quantum resilient encryption standards for the United States.<sup>93</sup> The administration should direct NIST to broaden the scope of its work to develop standards for QIS technology development and applications.<sup>94</sup>

The administration should develop DoD and Intelligence Community policy guidance to govern the sharing of QIS findings and capabilities with allies and partners. This guidance should be developed with representation from the Department of Commerce's National Telecommunications and Information Administration (NTIA) and NSF to balance security concerns with the benefits of collaboration; address government and private industry information, both classified and proprietary; and also should include categories of information that the United States is interested in receiving from allies and partners.

**Recommendation 2B.5: Establish a national QIS research, development, and testing infrastructure; fund quantum demonstration programs.**

The administration should establish a national QIS research, development, and testing infrastructure. This will comprise research centers focused on quantum computing, quantum communications, quantum sensing, and evaluation of QIS (including QIS-secure) applications; a national computational infrastructure to support this initiative;

- 90 William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021. SEC. 9414. *Study on Chinese Policies and Influence in the Development of International standards for Emerging Technologies* will produce an assessment of this issue for emerging technologies. SEC. 9414 is based on the "Ensuring American Leadership over International Standards Act of 2020," S. 4901, introduced on November 16, 2020, by Senator Cortez Masto (D-NV) and Senator Portman (R-OH), accessed March 26, 2021, <https://www.congress.gov/bill/116th-congress/senate-bill/4901/text> comprises.
- 91 "Working Group 14 for Quantum computing was established by ITO/IEC JTC1 in June 2020," JTC1, accessed March 26, 2021, <https://jtc1info.org/technology/working-groups/quantum-computing/>. IEC and ISO have set up a working group (WG 14) in their joint technical committee on information technology (JTC1) to identify the standardization needs of quantum computing.
- 92 "A 'China Model?' Beijing's Promotion of Alternative Global Norms and Standards," hearing before the U.S.-China Economic and Security Review Commission, 116th Congress, March 13, 2020, accessed March 26, 2021, [https://www.uscc.gov/sites/default/files/2020-10/March\\_13\\_Hearing\\_and\\_April\\_27\\_Roundtable\\_Transcript.pdf](https://www.uscc.gov/sites/default/files/2020-10/March_13_Hearing_and_April_27_Roundtable_Transcript.pdf).
- 93 National Institute of Standards and Technology, "NIST's Post-Quantum Cryptography Program Enters 'Selection Round,'" July 22, 2020, accessed March 26, 2021, <https://www.nist.gov/news-events/news/2020/07/nists-post-quantum-cryptography-program-enters-selection-round>.
- 94 Dr. Carl J. Williams, "NIST's Program in Quantum Information Science," accessed April 16, 2016, [https://science.osti.gov/-/media/nqiac/pdf/NIST\\_-presentation-NQIAC-20201027.pdf?la=en&hash=79A89EDF5BF6175360DF7EBCEB024F9B240B64A7](https://science.osti.gov/-/media/nqiac/pdf/NIST_-presentation-NQIAC-20201027.pdf?la=en&hash=79A89EDF5BF6175360DF7EBCEB024F9B240B64A7).

engineering testbeds; programs to build a skilled QIS workforce; and participation by private industry (for example, the Quantum Economic Development Consortium<sup>95</sup>) to advance the development of a national QIS infrastructure and create fielded capabilities. In support of the National Quantum Coordinating Office, an interagency group led by the Department of Energy, NIST, and DARPA should oversee this infrastructure initiative, coordinating federal programs and guiding private industry's participation.

The administration should develop demonstration programs that show, in operational settings, national security implications of near-term quantum platforms. Some examples include the following:

- **Quantum communications:** There are two areas of interest: (i) understanding vulnerabilities of various public key cryptographic systems to future quantum computing systems, an effort currently underway at NIST in the development of quantum resilient encryption standards, and (ii) use of QKD in large-scale demonstrations relevant to commercial and security applications, including space communications. QKD provides an approach to post-quantum communications security that is based on quantum phenomena, not algorithmic complexity.
- **Quantum computing:** Using small quantum computers in networked clusters or in hybrid architectures with classical computers.
- **Quantum networks:** The use of quantum networks for long-range quantum communications.
- **Quantum sensing:** Using quantum mechanics phenomena and devices for high-sensitivity and precision applications in sensing and communication, life sciences, and other fields.

The administration, through the National Quantum Coordinating Office, should establish funded competitions to improve the exchange of intellectual property and foster a common understanding across the government, industry, academic communities, and foreign institutions working on QIS.<sup>96</sup>

95 National Institute of Standards and Technology, "NIST Launches Consortium to Support Development of Quantum Industry," September 28, 2018, accessed March 25, 2021, <https://www.nist.gov/news-events/news/2018/09/nist-launches-consortium-support-development-quantum-industry>. The Quantum Economic Development Consortium (QEDC) is a public-private partnership in the United States tasked with developing the future workforce needs for the QIS economy. Virtually all of the US private sector quantum companies are represented in the QEDC.

96 J. Bienfang et al., *Building the Foundations for Quantum Industry*, NIST, June 20, 2018, accessed March 26, 2021, <https://www.nist.gov/system/files/documents/2018/06/20/report-on-qid-v10.pdf>.



## Chapter 3. Enhanced Trust and Confidence in the Digital Economy



Surgical team is seen during a by-pass implantation operation using the Da Vinci robot at the MSWiA (Ministry of Interior and Administration) hospital in Warsaw Poland, March 16, 2021. Artificial intelligence in the healthcare sector may rapidly expand the capabilities of robot-assisted surgery and other critical processes. Picture taken March 16, 2021.

Isaiah 66:10, 11  
© 2021 The Author(s)

**E**nhanced trust and confidence in the digital economy is founded upon personal privacy, data security, accountability for performance and adherence to standards, transparency of the internal decision-making algorithms, and regulations and governance for digital products and services. Trust and confidence in the digital economy is diminished by practices that do not protect privacy or secure data, and by a lack of legal and organizational governance to advance and enforce accountability.<sup>97</sup> Data breaches, malware embedded in downloaded apps, unfiltered mis- and disinformation, and the lack of governance models to effectively address these harms all contribute to the degradation of social and civic trust. This degradation

<sup>97</sup> Amon, "Toward a New Economy of Trust."

undermines economic and civic confidence, is costly,<sup>98</sup> constrains the growth of the digital economy,<sup>99</sup> and has destabilizing effects on society, governments, and markets. Trust and confidence in the digital economy is essential for open societies to function, and for resilience against cascading effects of local, regional, or national economic, security, or health instabilities.

**Finding 3: To enhance trust and confidence in artificial intelligence and other digital capabilities, technologies must objectively meet the public’s needs for privacy, security, transparency, and accountability.**

The growth of digital economies is changing how trust is valued by institutions, businesses, and the public.<sup>100</sup> The traditional view of trust is expressed in terms of the security of a business transaction. The increase in cyberattacks, identity theft, social media disinformation campaigns, and the use of autonomous decision-making software, introduces new factors that affect trust. Trust in a firm’s reputation and ethical practices, privacy protection, and how personal data are used depend on technology, business practices, and the public’s perception of how well these components of trust are protected.

Not everyone has the same perception of what is trustworthy. However, reaping the benefits of the digital economy requires a high level of trust among users. Therefore, government and industry should work to enhance the transparency and accountability of digital systems to improve trustworthiness. Challenges include the following: (i) views on personal privacy protection are context-dependent, vary by culture or location, and may be formalized in different terms across nations, regions, and states; and (ii) as automated decision-making algorithms proliferate, new applications reveal trust weaknesses regarding implicit bias, unethical use of personal data, and lack of identity protection.

Trustworthiness needs to be prioritized and empirically demonstrated in the evolving market. Building trust involves educating all participants on the fundamental value of

98 World Economic Forum, “Why trust in the digital economy is under threat,” accessed March 26, 2021, <http://reports.weforum.org/digital-transformation/building-trust-in-the-digital-economy/>, citing an estimate by McAfee that the costs associated with cybersecurity incidents approximated \$575 billion in 2014; Accenture, *Securing the Digital Economy: Reinventing the Internet for Trust*, 16, accessed March 26, 2021, [https://www.accenture.com/us-en/insights/cybersecurity/\\_acnmedia/Thought-Leadership-Assets/PDF/Accenture-Securing-the-Digital-Economy-Reinventing-the-Internet-for-Trust.pdf#zoom=50](https://www.accenture.com/us-en/insights/cybersecurity/_acnmedia/Thought-Leadership-Assets/PDF/Accenture-Securing-the-Digital-Economy-Reinventing-the-Internet-for-Trust.pdf#zoom=50). Cites five-year loss of foregone revenue from 2019 to 2023 to be \$5.2 trillion, calculated using a sample of 4,700 global public companies.

99 Congressional Research Service, *Digital Trade and U.S. Trade Policy*, 11, May 21, 2019, accessed March 26, 2021, <https://crsreports.congress.gov/product/pdf/R/R44565>; Alan B Davidson, “The Commerce Department’s Digital Economy Agenda,” Department of Commerce, November 9, 2015, accessed March 26, 2016, <https://2014-2017.commerce.gov/news/blog/2015/11/commerce-departments-digital-economy-agenda.html> Davidson identifies four pillars: promoting a free and open Internet worldwide; promoting trust online; ensuring access for workers, families, and companies; and promoting innovation.

100 Frank Dickson, “The Five Elements of the Future of Trust,” IDC, April 22, 2020, accessed March 26, 2021, <https://blogs.idc.com/2020/04/22/the-five-elements-of-the-future-of-trust/>.

trust in the digital economy and ensuring digital systems reflect individual and societal conceptions of trust. There must be national and international standards for judging how well technologies and systems protect trust. Professional organizations that audit for trust in the digital economy will strengthen accountability.

**Finding 3.1: The European Union's General Data Protection Regulation uses data protection rules as a trust-enabler.<sup>101</sup>**

As European Union (EU) member nations work to conform national rules and laws to the General Data Protection Regulation (GDPR), the European Commission notes that these steps may strengthen trust relationships. Other nations propose that a global framework for cross-border Internet policies may be able to protect data security and privacy while still allowing national laws and regulations as a part of the approach if certain trust relationships are maintained. For both approaches, a set of rules or principles provides the foundation for trust.

The GDPR<sup>102</sup> establishes regulations for data security and privacy that apply to any organization that collects or uses data related to people in the EU. The entire data chain is covered by the GDPR, including data collection, processing, storing, and managing.

The GDPR comprises principles that govern data protection and accountability for those who process data. There are technical measures for data security, and organizational design principles for data protection. Data privacy is expressed in terms of privacy rights, including the right: to be informed, to rectification, to erasure, to restrict processing, to data portability, and to object, and the right of access. There are also rights in relation to automated decision-making and profiling. The governance mechanism centers on Data Protection Authorities that work to align each EU member nation's approach to data security and privacy to conform with the GDPR. These Data Protection Authorities have enforcement powers and the ability to levy fines when a GDPR rule is violated.

**Finding 3.2: Current approaches to machine learning and big data analytics risk weakening data protection rules.<sup>103</sup>**

Data privacy protection is vulnerable to advanced data analytics that can infer personal identifiable information by joining loosely related data sources. As a result, the growing

101 "Communication from the Commission to the European Parliament and the Council. Data protection rules as a trust-enabler in the EU and beyond – taking stock," COM/2019/374 final, European Union, July 24, 2019, accessed March 26, 2021, <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2019:374:FIN>.

102 "General Data Protection Regulation." Intersoft Consulting, <https://gdpr-info.eu/>.

103 T. Timan and Z.Á. Mann, eds., *Data protection in the era of artificial intelligence. Trends, existing solutions and recommendations for privacy-preserving technologies*, Big Data Value Association, October 2019, accessed March 26, 2021, [https://www.bdva.eu/sites/default/files/Data%20protection%20in%20the%20era%20of%20big%20data%20for%20artificial%20intelligence\\_BDVA\\_FINAL.pdf](https://www.bdva.eu/sites/default/files/Data%20protection%20in%20the%20era%20of%20big%20data%20for%20artificial%20intelligence_BDVA_FINAL.pdf).

use of current machine learning methods applied to large, multi-source data sets highlights potential limitations in the GDPR where such computational methods can infer data originally made private. The development of new data science capabilities may require research on new privacy-preserving technologies for nations to remain compliant with the GDPR. With increasing amounts of personal medical and genetic information being held in data repositories, this need is urgent.

**Finding 3.3: Evolving US data privacy approaches consider outcome-based methods, versus prescriptive methods.**

The development of data privacy laws in the United States is an evolving patchwork, with more than one hundred and fifty state data privacy laws proposed in 2019.<sup>104</sup> There is no overall federal data privacy law.

One instance of federal legislation for data privacy proposed in the 117<sup>th</sup> Congress<sup>105</sup> includes the following key privacy features, which are viewed as outcome-based.<sup>106</sup>

- Transparent communication of the privacy and data use policy
- Affirmative opt-in and opt-out consent
- Preemption, in which the proposed statute would preempt most state laws with limited exceptions for data breaches, and other limited situations
- A right to action, enforced at the federal or state level, to address alleged violations
- Independent audit of the effectiveness and appropriateness of the privacy policy for each entity providing data services

Several bills<sup>107</sup> introduced in the 116<sup>th</sup> Congress addressed a subset of the above features or are focused on COVID-19 contact tracing, health status, and identifiers. In addition,

104 "2019 Consumer Data Privacy Legislation," National Conference of State Legislatures, January 3, 2020, accessed March 26, 2021, <https://www.ncsl.org/research/telecommunications-and-information-technology/consumer-data-privacy.aspx>.

105 "Information Transparency and Personal Data Control Act," fact sheet, accessed March 26, 2021, [https://delbene.house.gov/uploadedfiles/delbene\\_consumer\\_data\\_privacy\\_bill\\_fact\\_sheet.pdf](https://delbene.house.gov/uploadedfiles/delbene_consumer_data_privacy_bill_fact_sheet.pdf); Information Transparency & Personal Data Control Act, H.R. 2013 — 116th Congress (2019-2020), accessed April 2, 2021, [https://delbene.house.gov/uploadedfiles/delbene\\_privacy\\_bill\\_final.pdf](https://delbene.house.gov/uploadedfiles/delbene_privacy_bill_final.pdf).

106 "Developing the Administration's Approach to Consumer Privacy," *Federal Register*, September 26, 2018, accessed March 26, 2021, <https://www.federalregister.gov/documents/2018/09/26/2018-20941/developing-the-administrations-approach-to-consumer-privacy>; Alan Charles Raul and Christopher Fonzone, "The Trump Administration's Approach to Data Privacy, and Next Steps," Sidley Austin LLP, October 2, 2018, accessed March 26, 2021, <https://datamatters.sidley.com/the-trump-administrations-approach-to-data-privacy-and-next-steps>.

107 Setting an American Framework to Ensure Data Access, Transparency, and Accountability (SAFE DATA Act), S.4626 — 116th Congress (2019-2020), <https://www.congress.gov/116/bills/s4626/BILLS-116s4626is.pdf>; Online Privacy Act of 2019, H.R. 4978 — 116th Congress (2019-2020), <https://www.congress.gov/bills/116th-congress/house-bill/4978/text>; COVID-19 Consumer Data Protection Act of 2020, S. 3663 — 116th Congress (2019-2020), <https://www.congress.gov/bills/116th-congress/senate-bill/3663>.

several bills introduced in the 116<sup>th</sup> Congress addressed disclosing how data are used or monetized by social media companies that enhance the accessibility and portability of a user's data across devices.<sup>108</sup>

The National Institute of Standards and Technology (NIST) Privacy Framework describes a risk- and outcomes-based approach to establishing privacy protection practices in an organization. Organizations can vary the technologies and design of the privacy protection aimed at satisfying performance outcomes. This may be advantageous when the technologies and applications are changing at a fast pace, e.g., artificial intelligence (AI) and the Internet of Things (IoT).<sup>109</sup>

While there are several federal data privacy laws specific to certain industries or groups, e.g., the Health Insurance Portability and Accountability Act (HIPAA),<sup>110</sup> the eventual form and scope of US data protection laws will depend on policy and legal considerations. A key decision concerns the model for data protection laws. The EU GDPR model is prescriptive; GDPR compliance involves demonstrating that the procedural rules were followed. An alternate model for data protection laws is outcome-based, which allows flexibility in how to achieve data protection.<sup>111</sup>

A choice between prescriptive versus outcome-based approaches must assess their relative costs and benefits and how the two approaches can work together. The proposed bills in the 116<sup>th</sup> Congress identify a robust set of data privacy features while promoting flexibility and innovation in their implementation; the GDPR model has greater worldwide traction, creating opportunities for harmonized regulatory treatment.

### **Finding 3.4: New information technologies compel automated compliance testing.**

New information technologies and advanced data capabilities challenge current methods of compliance and enforcement. The variety of new ways to collect, process, and analyze

108 Designing Accounting Safeguards to Help Broaden Oversight and Regulations on Data Act, S. 1951 — 116th Congress (2019-2020), accessed March 26, 2021, <https://www.congress.gov/bill/116th-congress/senate-bill/1951>. The informal reference, DASHBOARD Act, is found in articles about this bill; Public Health Emergency Privacy Act, S. 3749 — 116th Congress (2019-2020), accessed March 26, 2021, <https://www.congress.gov/bill/116th-congress/senate-bill/3749>. This has been reintroduced in the 117th Congress. Mark R. Warner, Warner, Blumenthal, Eshoo, Schakowsky & DelBene Introduce the Public Health Emergency Privacy Act, press release, January 28, 2021, <https://www.warner.senate.gov/public/index.cfm/2021/1/warner-blumenthal-eshoo-schakowsky-delbene-introduce-the-public-health-emergency-privacy-act>; Augmenting Compatibility and Competition by Enabling Service Switching (ACCESS) Act of 2019, S. 2658 — 116th Congress (2019-2020), accessed March 26, 2021, <https://www.congress.gov/bill/116th-congress/senate-bill/2658>.

109 National Institute of Standards and Technology, "NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management, Version 1.0," January 16 2020, accessed March 26, 2021, [https://www.nist.gov/system/files/documents/2020/01/16/NIST%20Privacy%20Framework\\_V1.0.pdf](https://www.nist.gov/system/files/documents/2020/01/16/NIST%20Privacy%20Framework_V1.0.pdf).

110 Congressional Research Service, *Data Protection Law: An Overview*, March 25, 2019, accessed March 26, 2021, <https://fas.org/sgp/crs/misc/R45631.pdf>.

111 Ibid., 56.



data is increasing at a fast rate, while compliance often is determined on a case-by-case basis by regulatory and legal experts. To keep pace, automated testing for compliance with data privacy regulations is necessary.

Table 3 portrays some of the challenges and solutions for achieving automated compliance testing. This research agenda identifies the following key developments: standards, new privacy-preserving technologies, and automated methods to establish compliance.

**Table 3. Big Data Value Association Strategic Research and Innovation Agenda**

Challenges	Solutions
A general, easy-to-use, and enforceable data protection approach	Guidelines, standards, law, and codes of conduct
Maintaining robust data privacy with utility guarantees	Multiparty computation, federated learning approaches, and distributed ledger technologies
Risk-based approaches calibrating data controllers' obligations	Automated compliance, risk assessment tools
Combining different techniques for end-to-end data protection	Integration of approaches, toolboxes, overviews, and repositories of privacy-preserving technologies

*Source: Adapted from the authors.*

Privacy-preserving technologies are an active research area, and include the following:<sup>113</sup> secure multiparty computation, (fully) homomorphic encryption, trusted execution environments, differential privacy, and zero-knowledge proofs.

The value of privacy-preserving technologies involves trade-offs between privacy and utility—how useful is the resulting data—both of which are context dependent.<sup>114</sup> Affecting these trade-offs are the technical methods, the technical definitions of privacy, and the specifications of the privacy laws. The technical methods (e.g., anonymization, sanitization, and encryption) operate on data in different ways. The technical definition of privacy varies by application and the user's perceptions of risk versus the benefit of making personal data available. Privacy laws vary across nations, challenging the uniform application of technical methods. For both professionals and members of the public, making trade-offs between privacy and utility remains challenging. This is partially due to the absence of definitions of and standards for

112 Timan and Mann, Data protection.

113 Big Data UN Global Working Group, *UN Handbook on Privacy-Preserving Computation Techniques*, accessed March 26, 2021, <https://marketplace.officialstatistics.org/privacy-preserving-techniques-handbook>.

114 Daniel Bachlechner, Karolina La Fors, and Alan M. Sears, "The Role of Privacy-Preserving Technologies in the Age of Big Data," proceedings of the 13th Pre-ICIS Workshop on Information Security and Privacy, San Francisco, December 13, 2018, accessed March 26, 2021, [https://www.albany.edu/wisp/papers/WISP2018\\_paper\\_11.pdf](https://www.albany.edu/wisp/papers/WISP2018_paper_11.pdf); Felix T. Wu, "Defining Privacy and Utility in Data Sets," *University of Colorado Law Review* 84 (2013), accessed March 26, 2021, [http://lawreview.colorado.edu/wp-content/uploads/2013/11/13.-Wu\\_710\\_s.pdf](http://lawreview.colorado.edu/wp-content/uploads/2013/11/13.-Wu_710_s.pdf).

measuring privacy and the social benefits obtained from making data available for use by others.

**Finding 3.5: Trust and confidence in digital capabilities requires businesses and governments to focus on the responsible use of technology.**

Increasing trust and confidence in emerging technologies, such as AI, requires a recognition by both businesses and governments that they have an obligation to use technology responsibly, ensuring that technology has a positive impact on society, especially with regards to equality and inclusion.<sup>115</sup> Developing and innovating responsibly means ensuring that (i) ethical frameworks and policies exist to guide organizations during all aspects of a product's development and deployment, (ii) fairness in design is emphasized from the outset, and that (iii) questions around the manner in which technologies will be used are given the same rigorous examination as technical issues. As technological capabilities evolve and become more deeply intertwined in all aspects of society, businesses and governments must put ethics at the center of everything they do.

**Approach 3: Build in trust-enabling technologies, measure performance against standards, conduct independent compliance audits.**

The digital economy relies on achieving a high level of trust and confidence on a continuing basis as technologies evolve. Trust and confidence-enabling technologies must be developed and built into the components of the digital economy infrastructure; a detailed understanding of the trade-offs between privacy versus utility is an essential foundation. Such technologies must be paired with similar civic norms, practices, and rules designed to enhance confidence in the digital economy. To assure businesses that they remain compliant with data protection regulations as they modernize their practices, automated compliance testing, accompanied by standards of performance, is needed. To establish transparency for automated decision-making algorithms, standards for the measurable performance, i.e., the output results, are necessary. Independent assessments of the compliance testing and algorithmic transparency by professional auditing organizations could enhance trust among all participants in the digital economy and aid accountability and governance; such methods should be explored. However, mechanisms for compliance testing and auditing by regulators are also necessary.<sup>116</sup>

115 Kirsten Martin, Katie Shilton, and Jeffrey Smith, "Business and the Ethical Implications of Technology: Introduction to the Symposium," *Journal of Business Ethics* 160, 307–317 (2019), accessed April 16, 2021, <https://doi.org/10.1007/s10551-019-04213-9>

116 Nicholas Confessore, "Audit Approved of Facebook Policies, Even After Cambridge Analytica Leak," *New York Times*, April 19, 2018, accessed March 26, 2021, <https://www.nytimes.com/2018/04/19/technology/facebook-audit-cambridge-analytica.html>.

**Recommendation 3: Develop international standards and best practices for a trusted digital economy that accommodate national rules and regulations, streamline the process of independently assessing adherence to these standards.**

**Recommendation 3.1: Develop a US data privacy standard.**

Congress should create a national data privacy standard that embodies the following principles: (i) *appropriate use of data*: this defines the intended purpose for the collected data, the scope of what can be collected, the needed security, and the entities that are covered by the principle; (ii) *nondiscriminatory use*: the collected data cannot be used to discriminate against protected classes; (iii) *informed participation*: the individuals must receive the privacy policies in a transparent manner before data are collected, and provide affirmative express consent, including the ability to revoke consent and require destruction of the data or the movement of the data as directed by the individual (i.e., portability); (iv) *public reporting*: covered entities must periodically report on the data collected, retained, and destroyed, and the groups of individuals from whom the data were collected; (v) *independent audit*: the performance of covered entities with respect to the data privacy standard must be annually audited by an independent auditing organization, with parallel mechanisms to accommodate auditing and review by regulatory agencies; (vi) *enforcement*: federal and state enforcement organizations are given the authority to pursue violations of the laws for data privacy protection; (vii) *preemption*: this would preempt state privacy laws that are inconsistent with the proposed national standard; and (viii) *consumer protection laws*: the privacy standard would not interfere with consumer protection laws on issues apart from data privacy.

The data privacy standard should recognize gradations in the sensitivity of personal data—some personal data are treated more strictly than others. Affirmative express consent should be structured based on the types of data and how they will be used.

Congress should work to develop a national data privacy standard that can achieve global interoperability and should request an analysis of emerging privacy standards and issues that limit this achievement. Congress also should use the proposed national data privacy standard to inform the development of transparent national consumer data privacy laws that preserve individuals' control of their personal data and facilitate the development of trusted networks and applications.

The results should establish federal data privacy standards for personal data, establish standards for content moderation by information providers, and should regulate platform providers' ability to conduct experiments or surveys with users and user data without prior consent.

**Recommendation 3.2: Develop privacy-preserving technologies for the digital economy and demonstrate in a full-scale test their conformance with the General Data Protection Regulation.**

The administration should direct NIST to establish and test privacy-preserving technologies that enable a risk- and outcomes-based approach to trust in the digital economy. The test should evaluate, at scale, conformance with relevant GDPR rules, conformance with existing US laws governing data privacy, and robustness with respect to innovations and advances in information technologies and data capabilities, especially those based on AI, machine learning, and the IoT. This work should include the development of technical definitions of privacy and application-specific measures of the utility of analyses that are based on privacy-protected data. The tests should include end user evaluations.

The administration should establish a near-term program that demonstrates privacy-preserving technologies to aid the trusted collection and sharing of data for the purpose of improving individuals' access to healthcare during large-scale biological events. This program should be jointly managed by NIST, the Department of Health and Human Services (HHS), the National Institutes of Health (NIH), and the National Science Foundation (NSF). This program will monitor system performance to inform the development of standards for the ethical use of the shared data and how data governance will be formulated.

**Recommendation 3.3: Create measurement methods and standards for evaluating trust in the digital economy.**

The administration should direct the National Institute of Standards and Technology (NIST) to establish methods for evaluating users' trust in the digital economy given the increasing use of AI, big data analytics, and automated decision-making algorithms. This work builds on the Commission on Enhancing National Cybersecurity's *Report on Securing and Growing the Digital Economy*<sup>117</sup> and the *National Strategy for Trusted Identities in Cyberspace*.<sup>118</sup> One assessment framework example<sup>119</sup> describes measures of: "(i) user trust in the digital environment, e.g., data privacy, security, private sector efforts to control the spread of misinformation, and private sector adherence to cybersecurity best practices; (ii) the user experience, i.e., the effort needed to interact with

117 Commission on Enhancing National Cybersecurity, *Report on Securing and Growing the Digital Economy*, December 1, 2016, accessed March 26, 2021, <https://www.nist.gov/system/files/documents/2016/12/02/cybersecurity-commission-report-final-post.pdf>.

118 White House, "National Strategy for Trusted Identities in Cyberspace, Enhancing Online Choice, Efficiency, Security, and Privacy," April 2011, accessed March 26, 2021, [https://obamawhitehouse.archives.gov/sites/default/files/rss\\_viewer/NSTICstrategy\\_041511.pdf](https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf).

119 Bhaskar Chakravorti, Ajay Bhalla, and Ravi Shankar Chaturvedi, "How Digital Trust Varies Around the World," *Harvard Business Review*, February 25, 2021, accessed April 16, 2016, <https://hbr.org/2021/02/how-digital-trust-varies-around-the-world>.

the digital environment; (iii) user attitudes, e.g., how trusted are government and business leaders; and (iv) user behavior, i.e., how much do users interact with the digital environment.”<sup>120</sup>

The administration should create a coalition to develop international standards for achieving trust in the digital economy. The coalition should include representatives from NIST, the Federal Trade Commission (FTC), private industry, Federally Funded Research and Development Centers (FFRDCs), University Affiliated Research Centers (UARCs), and international standards organizations. The United States and like-minded nations and partners should develop national assessments of trust in the digital economy using these standards.

**Recommendation 3.4: Empower an organization to audit trust in the digital economy.**

Congress should establish or empower an organization to audit the efficacy of measures designed to ensure trust in the digital economy and assess conformance to current and future standards designed to enhance and maintain such trust. Independent third parties or the Government Accountability Office (GAO) are examples of where such auditing organizations could be housed.

As part of this process, the auditing organization could provide recommendations to Congress on legislation that would enhance existing trust measures, develop new trust measures, and create trust performance standards. The auditing organization should also provide a mechanism through which the public and industry can raise topics and concerns for attention and, for cases where assessments or audits were done, include an ombudsman function for assessment appeals, identification of new information, or adjudication of concerns in a manner distinct from political influence.

The administration should work to establish a similar auditing program with EU members of the International Organization of Supreme Audit Institutions.

**Recommendation 3.5: Assess standards relating to the trustworthiness of digital infrastructure.**

Congress should direct an assessment by the National Academies of Sciences, Engineering, and Medicine of the current national and international standards relating to the trustworthiness of digital infrastructure to support the digital economy. “Trustworthiness of an information system is defined as the degree to which an information system (including the information technology components that are used to build the system) can be expected to preserve the confidentiality, integrity, and availability of

<sup>120</sup> Appendix A provides several references on the topics of trust and countering digital misinformation.

the information being processed, stored, or transmitted by the system across the full range of threats.”<sup>121</sup>

Due to the increasing complexity of the digital infrastructure, the assessment should also review design standards for complex systems-of-systems from the perspective of trustworthiness. The overall assessment focuses on systems that support the digital economy. The study should assess the sufficiency of existing standards to guide improvements in trustworthiness, identify where new standards are needed, and recommend the data collection and testing methods that would enable ongoing assessments.

### **Recommendation 3.6: Educate the public on trustworthy digital information.**

Congress should establish a grant program led by NSF for the purpose of developing a curriculum on trustworthiness of information—distinct from the trustworthiness of information systems—in the digital age. This curriculum should be created by a consortium headed by a university or coalition of universities. The program should be administered by select universities, with the participation of US information providers. The goal should be to educate the public on how to assess the trustworthiness of information—its credibility, truthfulness, and authenticity, and to develop tools that students and members of the public can use and benefit from on a regular basis.

<sup>121</sup> National Institute of Standards and Technology, *Security and Privacy Controls for Information Systems and Organizations*, Special Publication 800-53, Revision 5, September 2020, accessed April 16, 2021, <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf>.

**Recommendation 3.7: Conduct demonstration projects involving artificial intelligence to improve delivery of public- and private-sector services at local, state, and federal levels.**

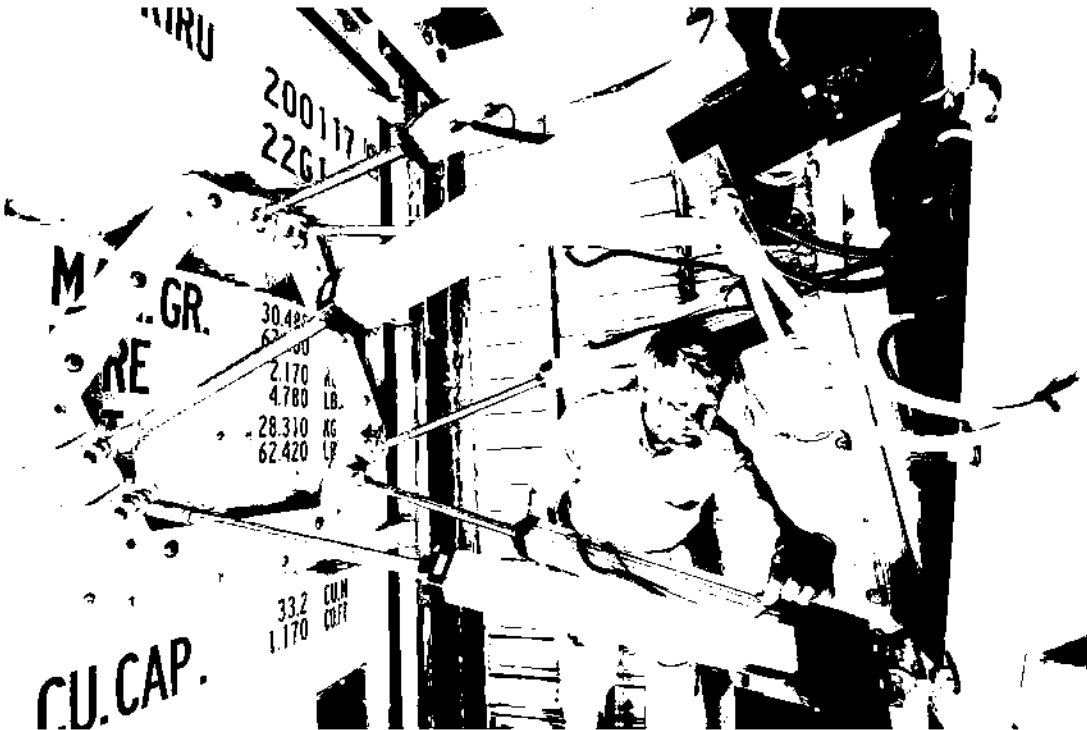
Congress should authorize and appropriate funds for AI demonstration projects that improve the delivery of public services.<sup>122</sup> The overall program would be managed by one of the National Laboratories or by a newly created FFRDC with the mission to leverage technology to improve the delivery of public services. These testbed projects would be supported by local and state grants, cross-cutting federal government efforts, and public-private partnerships (PPPs) to employ AI to improve healthcare, workforce training, food production and distribution, and other areas. The overarching goals are to increase public trust in, understanding of, and confidence in AI; to learn how to use AI in ways that reduce inequality and enhance, rather than replace, human work; and to improve access, affordability, and availability of such services. At local, state, and federal levels, individual government agencies will gain long-term benefits by acquiring the necessary data infrastructure to employ AI to improve the delivery of public services.

**Recommendation 3.8: Produce a framework for assessing ethical, social, trust, and governance considerations associated with specific current and future use cases for AI.**

The administration should request the National Academy of Sciences to produce a framework for assessing ethical, social, trust, and governance considerations associated with specific current and future use cases for AI solutions. The framework should identify where new federal standards and rules are needed. This guidance should be developed with the participation of relevant executive branch departments and agencies, and in consultation with private industry, academia, members of the public, and government and industry representatives from foreign partners.

122 A potential source for the types of initiatives of interest is the OECD Network of Experts on AI (ONE AI). This group provides policy, technical and business expert input to inform OECD analysis and recommendations. "OECD Network of Experts on AI (ONE AI)," OECD.AI, accessed March 26, 2021, <https://www.oecd.ai/network-of-experts>.

## Chapter 4. Assured Supply Chains and System Resiliency



Sandia National Laboratories Engineer John Dillinger tests the security of a cargo container. Testing and evaluating new cargo security technologies has been a partnership between Sandia, the Space and Naval Warfare Systems Command (SPAWAR) Systems Center Pacific (SSC Pacific) and the Department of Homeland Security (DHS).

SPAWAR photo by SA Dillinger

**B**oth physical and digital supply chain vulnerabilities can have cascading effects on the global economy and national security. Two critical examples include:

- **US dependence on foreign production of the main components used in generic drugs.** Trade disputes and economic crises can stop the flow of medicines and affect the health and economic welfare of tens of millions of individuals in the United States and other countries.<sup>123</sup>
- **US dependence on foreign-produced semiconductors for military and commercial products.** As the manufacturing and assembly of key components

<sup>123</sup> Congressional Research Service, *COVID-19: China Medical Supply Chains and Broader Trade Issues*, updated December 23, 2020, accessed March 26, 2021, <https://crsreports.congress.gov/product/pdf/R/R46304>.



shifts to markets in East Asia, particularly China,<sup>124</sup> the United States is susceptible to sudden interruptions in supplies and deliberate efforts to degrade the integrity of the products.

The interconnected global networks of manufacturing, transportation,<sup>125</sup> and distribution contain many instances where supply chain problems can have magnified effects. To protect against these diverse risks requires understanding which types of goods and sectors of the economy are critical. It also requires assessing the state and characteristics of supplies, trade networks and policies, inventory reserves, and the ability to substitute products or processing facilities. Assuring the performance of physical and software/IT supply chains is essential for a functioning, prosperous society and for national and economic security.

#### **Finding 4: Resilient, trusted supply chains require defense, diversification, and reinvention.**

One of the goals of the United States' National Strategy for Global Supply Chain Security<sup>126</sup> is to "foster a resilient supply chain." As part of its strategic approach, the national strategy works to prepare for, withstand, and recover from threats and disruptions. "Executive Order 13806 of July 21, 2017: Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States"<sup>127</sup> states that "a healthy manufacturing and defense industrial base and resilient supply chains are essential to the economic strength and national security of the United States" and requires a report detailing the current state of supply chains that are essential for national security. The Interagency Task Force report<sup>128</sup> in response to the executive order recommends decreasing the fragility and single points of failure of supply chains and diversifying away from dependencies on politically unstable countries.

It is difficult to know the full range of potential threats and disruptions for a given supply

124 Department of Defense, *Fiscal Year 2020: Industrial Capabilities: Report to Congress*, January 2021, accessed March 26, 2021, <https://media.defense.gov/2021/Jan/14/2002565311/-1/-1/0/FY20-INDUSTRIAL-CAPABILITIES-REPORT.PDF>.

125 Vivian Yee, "Ship Is Freed After a Costly Lesson in the Vulnerabilities of Sea Trade," *New York Times*, March 29, 2021, accessed April 3, 2021, <https://www.nytimes.com/2021/03/29/world/middleeast/suez-canal-ever-given.html>.

126 "National Strategy for Global Supply Chain Security," Department of Homeland Security, last published July 13, 2017, accessed March 26, 2021, <https://www.dhs.gov/national-strategy-global-supply-chain-security>.

127 "Executive Order 13806 of July 21, 2017: Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States," *Federal Register* 82 (142) (July 26, 2017), accessed March 26, 2021, <https://www.govinfo.gov/content/pkg/FR-2017-07-26/pdf/2017-15860.pdf>.

128 Department of Defense, *Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States. Report to President Donald J. Trump by the Interagency Task Force in Fulfillment of Executive Order 13806*, September 2018, accessed March 26, 2021, <https://media.defense.gov/2018/Oct/05/2002048904/-1/-1/1/ASSESSING-AND-STRENGTHENING-THE-MANUFACTURING-AND%20DEFENSE-INDUSTRIAL-BASE-AND-SUPPLY-CHAIN-RESILIENCY.PDF>.

chain. For multitiered supply chains, the primary suppliers may not have information on each of the suppliers at the third or fourth tier and will not have accurate or up-to-date information on the trustworthiness of the sources of components, e.g., circuit board component suppliers. The multiplying, dynamic effects of supply chain disturbances are often not deterministic. In cases of deliberate sabotage of a resource, there may not be observable indicators, as with the insertion of hidden back doors in software. Resilient supply chains address a portion of these uncertainties through risk-reduction strategies and greater supply chain transparency.

For some supply chains, resilience may be attained by increasing defenses through greater trade enforcement and strengthening key segments. For some supply chains, diversifying the sources and manufacturing locations, in partnership with allies, is an effective strategy. Adversaries are creating strategic vulnerabilities and weaknesses in US supply chains; a key area is the design and manufacture of advanced electronics. To address this growing risk, the strategy exemplified in the Defense Advanced Research Projects Agency's (DARPA's) Electronics Resurgence Initiative<sup>129</sup> involves developing new technologies for alternative materials, designs, and production processes.

#### **Finding 4.1: Critical supply chains are pervasive and challenging to defend.**

Presidential Policy Directive 21 (PPD-21), "Critical Infrastructure Security and Resilience," defines critical infrastructure to be those "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."<sup>130</sup> There are eighteen critical infrastructure sectors. The Sector-Specific Plans discuss critical infrastructure resilience and include the supply chains in the risk management or risk mitigation section of some sector plans.

Supply chain attacks can be hard to detect and defend against. The Department of Defense's (DoD's) report, *Department of Defense Strategy for Operating in Cyberspace*,<sup>131</sup> highlights the critical issue of supply chain vulnerabilities and the risks of US reliance on foreign suppliers. The range of supply chain attack opportunities is large—including design, manufacturing, servicing, distribution, and disposal segments of the supply chain—and challenging to detect.

129 "DARPA Electronics Resurgence Initiative," DARPA, last updated April 2, 2020, accessed March 26, 2021, <https://www.darpa.mil/work-with-us/electronics-resurgence-initiative>.

130 White House, "Presidential Policy Directive – Critical Infrastructure Security and Resilience," February 12, 2013, accessed March 26, 2021, <https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil>.

131 Department of Defense, "Department of Defense Strategy for Operating in Cyberspace," July 2011, accessed March 26, 2021, <https://csrc.nist.gov/CSRC/media/Projects/ISAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf>.

Appendix B discusses the cyberattack of FireEye, involving the theft of its penetration testing toolkit, and the breadth of a comprehensive cyber espionage campaign centered on SolarWinds' Orion network monitoring software. More than eighteen thousand commercial and government targets, including Intel, Microsoft, California state hospitals,<sup>132</sup> the National Nuclear Security Administration,<sup>133</sup> and dozens<sup>134</sup> of federal, state, and local government agencies, downloaded compromised updates, all with the goal of extracting valuable intelligence while remaining undetected.

#### **Finding 4.2: A broadened view of stockpiles increases resiliency.**

Creating additional supplies or increasing production capacity contribute to creating stockpiles in a supply network. Adding more production capacity in the United States, or encouraging allies to undertake similar actions, is the focus of recent legislative efforts.

The Coronavirus Aid, Relief, and Economic Security Act (CARES Act; P.L. 116-136) strengthened reporting requirements to delineate the domestic versus foreign production of finished drug products and active pharmaceutical ingredients. While the CARES Act requires the National Academies of Sciences, Engineering, and Medicine to evaluate the US medical product supply chain, options for increasing the security and resilience of this supply chain are still under consideration.<sup>135</sup>

The William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021<sup>136</sup> includes provisions to enhance the security of the semiconductor supply chain. It incentivizes investment in facilities and equipment in the United States for

132 Laura Hautala, "SolarWinds hackers accessed DHS acting secretary's emails: What you need to know," c|net, March 29, 2021, accessed April 16, 2021, <https://www.cnet.com/news/solarwinds-hackers-accessed-dhs-acting-secretarys-emails-what-you-need-to-know/>

133 Natasha Bertrand and Eric Wolff, "Nuclear weapons agency breached amid massive cyber onslaught," *Politico*, December 17, 2020, accessed March 26, 2021, <https://www.politico.com/news/2020/12/17/nuclear-agency-hacked-officials-inform-congress-447855>.

134 Raphael Satter, "U.S. cyber agency says SolarWinds hackers are 'impacting' state, local governments," Reuters, December 23, 2020, accessed March 26, 2021, <https://www.reuters.com/article/us-global-cyber-usa-idUSKB-N28Y09L>.

135 Congressional Research Service, *FDA's Role in the Medical Product Supply Chain and Considerations During COVID-19*, September 1, 2020, accessed March 26, 2021, <https://crsreports.congress.gov/product/pdf/R/R46507>.

136 Samuel K. Moore, "U.S. Takes Strategic Step to Onshore Electronics Manufacturing," *IEEE Spectrum*, January 6, 2021, "The semiconductor strategy and investment portion of the *William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021* began as separate bills in the House of Representatives and the Senate. In the Senate, it was called the American Foundries Act of 2020, and was introduced in July and called for \$15 billion for state-of-the-art construction or modernization and \$5 billion in R&D spending, including \$2 billion for the Defense Advanced Research Projects Agency's Electronics Resurgence Initiative. In the House, the *Creating Helpful Incentives to Produce Semiconductors (CHIPS) for America Act*, was introduced in the 116th Congress by Senators John Cornyn (R-TX) and Mark Warner (D-VA), and Representatives Michael McCaul (R-TX) and Doris Matsui (D-CA), and offered similar levels of R&D," accessed April 16, 2021, <https://spectrum.ieee.org/tech-talk/semiconductors/processors/us-takes-strategic-step-to-onshore-electronics-manufacturing>.

semiconductor fabrication, assembly, testing, advanced packaging, or R&D. It strengthens the United States' capacity to develop and produce cutting-edge semiconductors domestically through federal funding, promotes greater global transparency around subsidies to identify unfair or opaque forms of support that distort global supply chains, and provides funding support to "foreign government partners to participate in a consortium in order to promote consistency in policies related to microelectronics, greater transparency in microelectronic supply chains, and greater alignment in policies toward non-market economies."<sup>137</sup>

"Executive Order 13817 of December 20, 2017: A Federal Strategy to Ensure Secure and Reliable Supplies of Critical Minerals" defines "critical mineral" to be "(i) a non-fuel mineral or mineral material essential to the economic and national security of the United States, (ii) the supply chain of which is vulnerable to disruption, and (iii) that serves an essential function in the manufacturing of a product, the absence of which would have significant consequences for our economy or our national security."<sup>138</sup> Based on country production and import reliance, thirty-five minerals were deemed critical minerals.<sup>139</sup> For some of these critical minerals, increased domestic production is possible,<sup>140</sup> through the policies in the executive order intended to decrease the time to obtain mining permits.

The DoD is working to ensure reliable supplies of rare earth minerals by increasing domestic production and processing capabilities.<sup>141</sup> The department has taken steps to increase stockpiles, reduce reliance on Chinese sources, partner with private industry to increase production of rare earth magnets, and accelerate the development of new rare earth mineral processing technologies, and is seeking to increase funding for domestic production of rare earth minerals for munitions and missiles. To increase domestic production of rare earth minerals, mining-reform legislation is needed. The

137 US Sen. Mark R. Warner (D-VA), Bipartisan, Bicameral Bill Will Help Bring Production of Semiconductors, Critical to National Security, Back to U.S., press release, June 10, 2020, accessed March 26, 2021, <https://www.warner.senate.gov/public/index.cfm/2020/6/bipartisan-bicameral-bill-will-help-bring-production-of-semiconductors-critical-to-national-security-back-to-u-s>.

138 "Executive Order 13817 of December 20, 2017: A Federal Strategy To Ensure Secure and Reliable Supplies of Critical Minerals," *Federal Register*, December 20, 2017, accessed March 26, 2021, <https://www.federalregister.gov/documents/2017/12/26/2017-27899/a-federal-strategy-to-ensure-secure-and-reliable-supplies-of-critical-minerals>.

139 Aluminum (bauxite), antimony, arsenic, barite, beryllium, bismuth, cesium, chromium, cobalt, fluorspar, gallium, germanium, graphite (natural), hafnium, helium, indium, lithium, magnesium, manganese, niobium, platinum group metals, potash, the rare earth elements group, rhenium, rubidium, scandium, strontium, tantalum, tellurium, tin, titanium, tungsten, uranium, vanadium, and zirconium.

140 National Strategic and Critical Minerals Production Act, H.R. 2531 — 116th Congress (2019-2020), accessed March 26, 2021, <https://www.congress.gov/bill/116th-congress/house-bill/2531>. The bill aims to increase the domestic supply of critical minerals.

141 Department of Defense, DOD Announces Rare Earth Element Awards to Strengthen Domestic Industrial Base, press release, November 17, 2020, accessed March 26, 2021, <https://www.defense.gov/Newsroom/Releases/Release/Article/2418542/dod-announces-rare-earth-element-awards-to-strengthen-domestic-industrial-base/>.

current mine-permitting process takes approximately ten years, when timelines of two to three years may be possible. Cooperative agreements with like-minded countries may also increase the supply available to the United States. South Africa, Canada, Australia, Brazil, India, Malaysia, and Malawi have rare earth minerals; China, Russia, and the United States hold 82.6 percent of the world's production and reserves.<sup>142</sup>

**Finding 4.3: By creating new materials and new design and manufacturing technologies, the United States can eliminate critical dependencies on foreign sources.**

The DARPA Electronics Resurgence Initiative<sup>143</sup> is in the fourth year of a long-term, \$1.5 billion effort to reinvent defense electronics both to improve performance and to respond to foreign efforts to shift innovation in electronics away from the United States. The program currently includes applications of the new materials, chip designs, chip manufacturing technologies, and new methods for increasing security in a variety of defense systems. At present, the United States imports 80 percent of its rare earth elements directly from China.

The DARPA Electronics Resurgence Initiative supports the goals of the “Executive Order 13953 of September 30, 2020: Addressing the Threat to the Domestic Supply Chain From Reliance on Critical Minerals From Foreign Adversaries and Supporting the Domestic Mining and Processing Industries.” The transformation of microelectronics is DoD’s top modernization priority. A critical, fundamental risk is the US dependence on foreign semiconductor chip manufacturing, dominated by microelectronics fabrication plants in vulnerable Taiwan and South Korea.

**Approach 4: Develop supply chain resilience strategies for a broadened set of critical resources, conduct assessments with allies.**

The United States must establish criteria for determining which supply chains are critical and develop supply chain assurance strategies based on knowledge of the current supply network and the creation of alternative pathways, processes, and materials. Such strategies must incorporate (i) a supplier nation’s trade and export policies and the effects of sudden changes, (ii) a nation’s near-monopoly of a key resource, (iii) alternate supply lines available to the United States, (iv) baseline capacities and resources, and (v) the ability to reestablish commercial operations in locations having lower risk.<sup>144</sup>

142 Marc Humphries, *Rare Earth Elements: The Global Supply Chain*, Congressional Research Service, December 16, 2013, accessed March 26, 2021, <https://fas.org/sgp/crs/natsec/R41347.pdf>.

143 “DARPA Electronics Resurgence Initiative,” DARPA.

144 Congressional Research Service, *COVID-19: China Medical Supply Chains and Broader Trade Issues*, R46304, April 6, 2020, updated December 23, 2020, accessed March 26, 2021, <https://crsreports.congress.gov/product/pdf/R/R46304>.

For information systems and networks, the United States should develop and test cybersecurity resilience strategies and performance standards for increased cybersecurity in systems that support supply chains for critical resources.

**Recommendation 4: Conduct regularized assessments in the United States and in allied countries to determine critical supply chain resilience and trust, implement risk-based assurance measures. Establish coordinated cybersecurity acquisition across government networks and create more experts.**

**Recommendation 4.1: Implement a framework that identifies and establishes global data collection on critical resources.**

“Executive Order 14017 of February 24, 2021: America’s Supply Chains,” will conduct a review of critical supply chain vulnerabilities affecting both government procurement and also that of the private sector. This review will address the changing nature of critical supply chains as “manufacturing and other needed capacities of the United States modernize to meet future needs.”<sup>145</sup> It will examine dependence on foreign suppliers, measures of resilience, and a range of sectors including energy, semiconductors, key electronics and related technologies, telecommunications infrastructure, and key raw materials. Strategies to increase critical supply chain resilience include “a combination of increased domestic production, strategic stockpiles sized to meet our needs, cracking down on anti-competitive practices that threaten supply chains, implementing smart plans to surge capacity in a time of crisis, and working closely with allies.”<sup>146</sup> After this initial review, the administration plans to ask Congress to enact a mandatory quadrennial critical supply chain review to institute this process permanently.

To conduct this critical supply chain review, the administration should develop a set of criteria for determining resources that are critical to the nation with respect to public health, national security, economic security, and technological competitiveness. These criteria should encompass critical resources beyond high-technology products, to include IT and computer systems and infrastructures, and lower technology products that are important for high-technology competitiveness, e.g., steel, auto parts, and other portions of US manufacturing industries. These criteria should be developed by the White House Office of Science and Technology Policy (OSTP) in coordination with relevant executive branch agencies and departments and with

145 “Executive Order on America’s Supply Chains,” White House, February 24, 2021, accessed March 26, 2021, <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/02/24/executive-order-on-americas-supply-chains/>; “Executive Order 14017 of February 24, 2021, America’s Supply Chains,” *Federal Register*, March 1, 2021, <https://www.federalregister.gov/documents/2021/03/01/2021-04280/americas-supply-chains>.

146 “The Biden Plan to Rebuild U.S. Supply Chains and Ensure the U.S. Does Not Face Future Shortages of Critical Equipment,” accessed March 26, 2021, <https://joebiden.com/supplychains/>.

the active participation of private industry. Because critical resources are dynamic in nature and are constantly evolving, this should be a recurring, ongoing initiative.

The administration should use existing fora for international outreach to foster data collection and information sharing for assessments of critical resources and critical supply chains. It should also identify where US funding will strengthen supply chain assurance in partner countries, particularly those with a strong rule of law and a commitment to intellectual property protection. The assessments must address where key resources (e.g., pharmaceuticals,<sup>147</sup> agricultural products<sup>148</sup>) are manufactured and sourced, and how this impacts the robustness of US supply chains, the ability to manufacture the key resources in the United States, and other issues concerning supply chain threats and vulnerabilities. The United States-Mexico-Canada Agreement (USMCA) in its “Rules of Origin” chapter provides a model for agreements with like-minded countries.<sup>149</sup> The United States Trade Representative would develop trade agreements that help strengthen supply chains.

**Recommendation 4.2: Fund and broaden federal oversight of supply chain assurance to include all critical resources.**

Congress should establish an annual reporting requirement that assesses the supply chain assurance for all critical resources, to be assigned to the Department of Homeland Security (DHS) with support from the Office of Management and Budget (OMB). The Cybersecurity and Infrastructure Security Agency (CISA) will contribute assessments of the cybersecurity of the supply chains included in the annual report. This report should determine priorities for supply chains deemed critical to US national and economic security and national health. Congress should require that federal budget requests affecting critical supply chains are based on these priorities.

The administration should develop an approach to address risk management for supply chains beyond those already associated with information technology and computer systems. The administration should extend the work by NIST to model critical assets

147 OECD and European Union Intellectual Property Office, *Trade in Counterfeit Pharmaceutical Products*. (Paris: OECD Publishing, 2020), accessed March 26, 2021, <https://doi.org/10.1787/a7c7e054-en>; Agnes Shanley, “Focusing on the Last Link,” *PharmaTech*, September 2, 2018, accessed March 26, 2021, <https://www.pharmtech.com/view/focusing-last-link>; *Eurohealth*, Quarterly of the European Observatory on Health Systems and Policies 24 (3) (2018), accessed March 26, 2021, [https://www.euro.who.int/\\_\\_data/assets/pdf\\_file/0011/382682/eurohealth-vol24-no3-2018-eng.pdf?ua=1](https://www.euro.who.int/__data/assets/pdf_file/0011/382682/eurohealth-vol24-no3-2018-eng.pdf?ua=1).

148 Clara Frezal and Grégoire Garsous, “New digital technologies to tackle trade in illegal pesticides,” OECD Trade and Environment Working Papers 2020/02, OECD Publishing, accessed March 26, 2021, <https://doi.org/10.1787/9383b310-en>.

149 “Agreement between the United States of America, the United Mexican States, and Canada 7/1/20 Text,” Office of the United States Trade Representative, accessed March 26, 2021, <https://ustr.gov/trade-agreements/free-trade-agreements/united-states-mexico-canada-agreement/agreement-between/>.

and components for information systems,<sup>150</sup> to critical resources as described here. This effort will delineate the data—for both physical supply chains and software/IT supply chains—required to perform supply chain assurance assessments.

**Recommendation 4.3: For the United States, the administration must develop a geopolitical deterrence strategy that addresses critical digital resources and digital supply chain assurance.**

State-based cyber-enabled threats to the integrity of global supply chains—impacting both physical (as seen in disruption to global logistics and manufacturing activity in the wake of the NotPetya ransomware attack<sup>151</sup>) and digital (as illustrated in the wake of the SolarWinds compromise) supply chains—increasingly represent costly and high-impact challenges. The national cyber director, as part of the National Cyber Strategy, should develop a geopolitical deterrence strategy that enables the US government to leverage all tools of US power—from diplomacy, to sanctions, cyber, and military activity—to exercise deterrence. The administration should evaluate the potential for (i) continuous evaluation of digital supply chains to enable prompt detection of malicious activity targeting these supply chains, and (ii) prompt detection, combined with improved supply chain resilience and timely actions in response to the detected activity, to decrease the likelihood of cyberattacks. Continuous evaluation of supply chains for critical digital resources<sup>152</sup> would be coordinated and managed by CISA as part of its role in managing federal cybersecurity risk.

**Recommendation 4.4: Conduct regular physical and software/IT supply chain assessments in the United States and with allies, focused on intersecting vulnerabilities with cascading consequences.**

The administration should establish with allies and partner nations a test program for supply chains and reporting on supply chains' status and test results. This reporting would address the readiness status of both public and private sector supply chains, and the results of exercises that test the preparedness, adequacy, and resiliency of supply chains against a range of conditions and scenarios, much like stress tests for the financial sector.

- Because most of the supply chain data are held by private companies, a key issue is whether the private sector will provide enough data about its supply

150 "NISTIR 8179, Criticality Analysis Process Model: Helping Organizations Decide Which Assets Need to Be Secured First," National Institute of Standards and Technology, April 11, 2018, accessed March 26, 2021, <https://csrc.nist.gov/News/2018/NISTIR-8179-Criticality-Analysis-Process-Model>.

151 Andy Greenberg, "The Untold Story of NotPetya, the most Devastating Cyberattack in History," *Wired*, August 22, 2018, accessed March 26, 2021, <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/>.

152 A key enabler of continuous evaluation comprises software configuration databases which will permit visibility and traceability of software/IT supply chains. These require development.



chains, or can be incentivized to do so. Questions to address include: what is the minimal information that is needed to calculate these performance measures, and will the resultant tests provide useful results across the situations of interest? will the private sector give these data, given its competitive positions? what is the best estimate of the metrics subject to the data availability constraints? Thus, the tests must show these estimates can be developed using acceptable access to the private data, or must determine a narrower set of criteria to test against.

Due to the many factors bearing on cybersecurity resilience, including the growing threat of sophisticated cyberattacks by major adversaries, the administration should develop software/IT supply chain resilience risk assessments that incorporate the effects of new standards and tools to measure cyber vulnerabilities, improved information sharing (including intelligence information on nation state-supported cyberattacks and ransomware denial of service attacks), designs for improvements that protect against systemic vulnerabilities, and new technologies such as cloud-based services.

## Chapter 5. Continuous Global Health Protection and Global Wellness



People receive their coronavirus disease (COVID-19) vaccines at a mass vaccination site at Lumen Field Event Center in Seattle, Washington, U.S. March 13, 2021.

**T**he COVID-19 pandemic has disrupted health and economic security, both directly and indirectly, for most of the planet. Inherent to this disruption are three systemic problems: (i) global and national leaders acted slowly to detect and contain the spread of the virus, (ii) global health organizations reacted slowly to contain the spread of the virus, and (iii) a mixture of factors caused the delayed response including late recognition of the threat and where it was circulating, slow incorporation of science and data into decision making, poor political will, and inconsistent messaging to citizens regarding the nature of the threat and precautions to take. The origin and spread of the coronavirus that causes COVID-19 also depended on a number of codependent factors—human encroachment on animal habitats, globalization and an interconnected world, and a global economy that ignored insufficient sanitation and public health standards. But, most importantly, it depended on a failure of adequate monitoring, data sharing, and early warning and mitigation systems.

Viruses and other pathogens know no borders, nor do they discriminate by race or

class. Though nations may adopt their own strategies to enhance resilience and future planning, a more global approach to this interconnected system will be essential to keep all humans safe. Continuous global health protection builds upon a foundation of secure data and communications, rapid sharing of biological threat data across the globe, enhanced trust and confidence in the digital economy, and assured supply chains.

**Finding 5: There is a need for a continuous biological surveillance, detection, and prevention capability.**

The design of a pandemic surveillance, detection, and prevention system would require a multipronged approach, comprising global monitoring, early detection, rapid warning, and capable mitigation and prevention strategies. The system would perform the following main functions: biothreat agent recognition, mobilization of defenses, containing the spread of the biothreat agent, administration of therapeutic treatment, and the ability to recognize new pathogens and form specific neutralizing responses.

Much of the integrative assessments performed by the system would need to rely on a network capable of receiving data from multiple, decentralized information sources, and converting that information into indicators that can be aggregated and evaluated to support decision making at the individual, local community, and population level.<sup>153</sup> A global detection and response system could enable greater resilience and prevention, and decrease the potential that new outbreaks of pathogens lead to global pandemics.<sup>154</sup>

**Finding 5.1: An early detection and warning system<sup>155</sup> requires global data collection of pathogen-related indicators, sometimes requiring novel sources to address information gaps.**

Early detection would require the funding of a global, interconnected system that relies on partnerships among national governments and regional partners. Where there are gaps in collecting and sharing preferred data, e.g., when a nation or region

153 National Syndromic Surveillance Program, "North Carolina Integrates Data from Disaster Medical Assistance Teams for Improved Situational Awareness," Centers for Disease Control and Prevention, accessed March 26, 2021, <https://www.cdc.gov/nssp/success-stories/NC-Disaster-Teams.html>; "Influenza - Surveillance and monitoring," World Health Organization, accessed March 26, 2021, [https://www.who.int/influenza/surveillance\\_monitoring/en/](https://www.who.int/influenza/surveillance_monitoring/en/).

154 "World Health Organization, Global Influenza Surveillance and Response System," World Health Organization, accessed March 26, 2021, [https://www.who.int/influenza/gisrs\\_laboratory/updates/GISRS\\_one\\_pager\\_2018\\_EN.pdf?ua=1](https://www.who.int/influenza/gisrs_laboratory/updates/GISRS_one_pager_2018_EN.pdf?ua=1).

155 "Toward the Development of Disease Early Warning Systems," in *Under the Weather: Climate, Ecosystems, and Infectious Disease*, National Research Council (US) Committee on Climate, Ecosystems, Infectious Diseases, and Human Health [Washington, DC: National Academies Press (US), 2001], <https://www.ncbi.nlm.nih.gov/books/NBK222241/>.

does not participate, alternative indicators would need to be developed.<sup>156</sup>

The development of novel, authenticated data sources is a key risk factor for pandemic warning systems. As seen at the start of the COVID-19 pandemic, relying on government-provided information led to a delay in identifying the unusual pneumonia-like illness in Wuhan, China, and ultimately in releasing the genetic sequence of the virus.<sup>157</sup> It cost lives, delayed warnings and the ability for others to detect the circulating virus, delayed containment and mitigation strategies (e.g., vaccine and therapeutic development), and enabled the virus to spread globally via human vectors.<sup>158</sup>

Authenticated data sources from different decentralized sources and edge devices could include both traditional (e.g., positive viral tests, hospitalization rates, excess death rates) and nontraditional sources of health information (e.g., passive monitoring of environment, wastewater, satellite data, human migration trends, market signals) that can be overlaid, combined, and aggregated to understand current public health conditions and to have predictive value.

## **Finding 5.2: An elevated capacity on the global stage is required.**

The components of global capacity in a pandemic include the ability to quickly identify and sequence novel pathogens; to quickly share that information with the world; to rapidly ramp-up testing; to develop and approve targeted vaccines and therapeutics; to have medical supply chain, manufacturing, and distribution capabilities in place; to have sufficient capital health equipment, medical consumables, and healthcare personnel in place; and to provide access to healthcare and reliable health information to all those in need.

- 156 Sylvia Mathews Burwell et al., "Improving Pandemic Preparedness: Lessons From COVID-19," Independent Task Force Report No. 78, Council on Foreign Relations, October 2020, accessed March 26, 2021, [https://www.cfr.org/report/pandemic-preparedness-lessons-COVID-19/pdf/TFR\\_Pandemic\\_Preparedness.pdf](https://www.cfr.org/report/pandemic-preparedness-lessons-COVID-19/pdf/TFR_Pandemic_Preparedness.pdf); Elias Kondilis et al., "COVID-19 data gaps and lack of transparency undermine pandemic response," *Journal of Public Health*, February 9, 2021, fdab016, <https://doi.org/10.1093/pubmed/fdab016>; Kamran Ahmed et al., "Novel Approach to Support Rapid Data Collection, Management, and Visualization During the COVID-19 Outbreak Response in the World Health Organization African Region: Development of a Data Summarization and Visualization Tool," *JMIR Public Health and Surveillance* 6 (4) (Oct-Dec, 2020), accessed March 26, 2021, <https://publichealth.jmir.org/2020/4/e20355/>; Sameer Saran et al., "Review of Geospatial Technology for Infectious Disease Surveillance: Use Case on COVID-19," *Journal of the Indian Society of Remote Sensing* 48 (2020): 1121-1138, accessed March 26, 2021, <https://doi.org/10.1007/s12524-020-01140-5>.
- 157 Associated Press, "China didn't warn public of likely pandemic for 6 key days," April 15, 2020, accessed March 26, 2021, <https://apnews.com/68a9e1b91de4ffc166acd6012d82c2f9>.
- 158 Jin Wu et al., "How the Virus Got Out," *New York Times*, March 22, 2020, accessed March 26, 2021, <https://www.nytimes.com/interactive/2020/03/22/world/coronavirus-spread.html>; Zhidong Cao et al., "Incorporating Human Movement Data to Improve Epidemiological Estimates for 2019-nCoV," medRxiv, <https://doi.org/10.1101/2020.02.07.20021071>

These specific functions for creating a comprehensive global alert and response system and coordinating actions, as well as supporting localized capacity strengthening,<sup>159</sup> were made part of the World Health Organization's (WHO's) updated 2005 International Health Regulations (IHR)<sup>160</sup> and its pandemic preparedness plan.<sup>161</sup> "To help countries review and, if necessary, strengthen their ability to detect, assess, and respond to public health events, WHO develops guidelines, technical materials, and training and fosters networks for sharing expertise and best practices. WHO's help supports countries in meeting their commitments under the IHR to build capacity for all kinds of public health events."<sup>162</sup>

To achieve the fullest potential of these approaches, there need to be investments on a global scale to support expanded detection, mitigation, and capacity-building strategies. These efforts should be conducted through public, private, and government partnerships based on mutual agreements to share data and report issues early. These should be multinational collaborations that would be able to overcome the limiting factors discussed in the next section. In developing these approaches, a priority is to strengthen transparency and accountability within the United Nations (UN) system, including at the WHO.<sup>163</sup>

### **Finding 5.3: There are several limiting factors.**

There often is a lack of trust among groups, institutions, and governments. Governments do not always trust other governments; countries do not always trust global health bodies; nationally, states do not always trust each other or the federal government; and individuals do not always trust governments or health entities or officials. This lack of trust is well-documented. According to the 2020 Edelman Trust

159 "Strengthening health security by implementing the International Health Regulations (2005), Country capacity strengthening," UN World Health Organization, accessed March 26, 2021, <https://www.who.int/ihr/capacity-strengthening/en/>.

160 "Strengthening health security by implementing the International Health Regulations (2005), A global system for alert and response," World Health Organization, [https://www.who.int/ihr/alert\\_and\\_response/en/](https://www.who.int/ihr/alert_and_response/en/); Apoorva Mandavilli, "239 Experts With One Big Claim: the Coronavirus Is Airborne," *New York Times*, updated November 19, 2020, accessed March 26, 2021, <https://www.nytimes.com/2020/07/04/health/239-experts-with-one-big-claim-the-coronavirus-is-airborne.html>.

161 World Health Organization, *WHO global influenza preparedness plan: The role of WHO and recommendations for national measures before and during pandemics*, 2005, accessed March 26, 2021, [https://www.who.int/csr/resources/publications/influenza/WHO\\_CDS\\_CSR\\_GIP\\_2005\\_5.pdf](https://www.who.int/csr/resources/publications/influenza/WHO_CDS_CSR_GIP_2005_5.pdf).

162 "Strengthening health security by implementing the International Health Regulations (2005), Country capacity strengthening," UN World Health Organization, accessed March 26, 2021, <https://www.who.int/ihr/capacity-strengthening/en/>.

163 Chairman Michael McCaul. *China Task Force Report*, U.S. House of Representatives, 116th Congress, September 2020, accessed March 26, 2021, <https://gop-foreignaffairs.house.gov/wp-content/uploads/2020/09/CHINA-TASK-FORCE-REPORT-FINAL-9.30.20.pdf>.

Barometer,<sup>164</sup> “no institution is seen as both competent and ethical,” an opinion that includes government, business, nongovernmental organizations (NGOs), and the media. In the statistical model Edelman provides, government is widely seen as the most unethical, and the least competent, institution of the four. According to the International Development Association of the World Bank Group, half of the global population does not trust government institutions.<sup>165</sup> Similarly, both individual citizens and countries may lack trust in national and global health bodies.

Health institutions are concerned about sharing data on health outbreaks too early, as this could make them look underinformed, or to be “crying wolf” before the true measure of an outbreak is known.<sup>166</sup> Governments may be incentivized to withhold information on outbreaks to maintain appearances of strength and ultimately to control medical supplies to keep their own people safe. Withholding immediate access to information can severely affect outcomes, such as the spread of the virus, allowing it to gain a foothold in other countries unaware. It also prevents the type of global and interdisciplinary cross-collaboration that has been so effective at advancing science, research and development (R&D), and progress toward solutions.

The cost of developing and operating a global pandemic surveillance, detection, and warning and response system must be borne by all nations in an equitable manner. A recent study<sup>167</sup> estimates “[t]his cost includes the cumulative cost of failed vaccine candidates through the research and development process. ... [P]rogressing at least one vaccine through to the end of phase 2a for each of the 11 epidemic infectious diseases would cost a minimum of \$2.8–3.7 billion (\$1.2 billion–\$8.4 billion range).” According to a 2002 study, the cost of developing a vaccine—from research and discovery to product registration—is estimated to be between \$200 million and \$500 million per vaccine.<sup>168</sup> Due to the high costs of developing vaccines and current therapeutics, developing an equitable funding model will rely on new research to make vaccines less expensive to develop, new technologies to conduct wide-area detection of signatures of biological activity, and new techniques for inexpensive diagnostic testing worldwide. The supply

164 “2020 Edelman Trust Barometer,” Edelman, accessed March 26, 2021, <https://www.edelman.com/trust/2020-trust-barometer>.

165 “Governance and Institutions,” International Development Association, World Bank Group, accessed March 26, 2021, <https://ida.worldbank.org/theme/governance-and-institutions>.

166 Stephen Buranyi, “The WHO v coronavirus: why it can’t handle the pandemic,” *Guardian*, April 10, 2020, accessed March 26, 2021, <https://www.theguardian.com/news/2020/apr/10/world-health-organization-who-v-coronavirus-why-it-cant-handle-pandemic>.

167 Dimitrios Gouglas et al., “Estimating the cost of vaccine development against epidemic infectious diseases: a cost minimisation study,” *Lancet Global Health* 6 (12) (E1386–E1396, DECEMBER 01, 2018), October 17, 2018, DOI: [https://www.thelancet.com/journals/langlo/article/PIIS2214-109X\(18\)30346-2/fulltext](https://www.thelancet.com/journals/langlo/article/PIIS2214-109X(18)30346-2/fulltext), accessed March 26, 2021.

168 Irina Serdobova and Marie-Paule Kieny, “Assembling a Global Vaccine Development Pipeline for Infectious Diseases in the Developing World,” *American Journal of Public Health* 96 (9): 1554–1559, <https://doi.org/10.2105/AJPH.2005.074583>, accessed March 26, 2021.

chains, manufacturing capabilities, vaccines, and therapeutics must be developed in such a manner that all nations are protected by such a global pandemic prevention system. The concern extends beyond vaccines which have been developed. Some diseases, like Zika, for which no vaccines exist, continue to be studied; and parasites, such as those that cause malaria, may become more widespread due to global climate change.

There are many types and sources of data that need to be identified in order to effectively predict or fight an epidemic. One is vector tracking. It is difficult to track zoonotic vectors that lead to viral spread. It is estimated that wild animals, in particular mammals, harbor an estimated forty thousand unknown viruses, a quarter of which could potentially jump to humans;<sup>169</sup> it is also estimated that 75 percent of all emerging pathogens in the last decade have come from a zoonotic event.<sup>170</sup> Further, it is complicated to surveil and track pathogen genesis, evolution, and global spread. Understanding of the science of viruses, other pathogens, and their mutation and evolution is incomplete, and research continues on new ways to monitor and spot outbreaks.

Insufficient public health infrastructures. A 2017 study conducted by the World Bank and the WHO points out that half of the global population does not have access<sup>171</sup> to necessary health services, and one hundred million people live in extreme poverty.<sup>172</sup>

### **Approach 5: Develop a global pandemic surveillance, detection, and response system based on data sensing and integration via trusted networks.**

Three important elements of this global system are the early detection and warning system, the rapid response and recovery system, and the elevated capacity building system.

169 C.J. Carlson et al., "Global estimates of mammalian viral diversity accounting for host sharing," *Nature Ecology & Evolution* 3 (2019): 1070-1075 (2019), <https://doi.org/10.1038/s41559-019-0910-6>, accessed March 26, 2021. Global Virome Project / PREDICT has estimated that there are over 1.6 million unknown viral species in mammalian and avian populations, of which approximately 700,000 have the potential to infect and cause disease in humans. "Global Virome Project," <https://static1.squarespace.com/static/581a4a856b8f5bc98311fb03/t/5ada612470a6ad672eea01b3/1524261157638/GVP%2B2%2Bpaper%2BFINAL.pdf>.

170 Alex Long, "Zoonotic Diseases and the Possibilities with EBV Monitoring," *CTRL Forward*, November 14, 2017, accessed March 26, 2021, <https://www.wilsoncenter.org/blog-post/zoonotic-diseases-and-the-possibilities-ebv-monitoring>.

171 World Health Organization, "World Bank and WHO: Half the world lacks access to essential health services, 100 million still pushed into extreme poverty because of health expenses," December 13, 2017, accessed March 26, 2021, <https://www.who.int/news-room/detail/13-12-2017-world-bank-and-who-half-the-world-lacks-access-to-essential-health-services-100-million-still-pushed-into-extreme-poverty-because-of-health-expenses>.

172 "Health Financing: Key policy messages," World Health Organization, accessed March 26, 2021, [https://www.who.int/health\\_financing/topics/financial-protection/key-policy-messages/en/](https://www.who.int/health_financing/topics/financial-protection/key-policy-messages/en/).

**Recommendation 5: Field and test new approaches that enable the world to accelerate the detection of biothreat agents, to universalize treatment methods, and to engage in mass remediation through multiple global means.**

**Recommendation 5.1: Develop a global early warning system comprised of pandemic surveillance systems coupled with an early warning strategy.**

Congress should request the Centers for Disease Control and Prevention (CDC), National Institutes of Health (NIH), United States Agency for International Development (USAID), United States Department of Agriculture (USDA), and other associated agencies to jointly develop an initial demonstration of this system in collaboration with the WHO, private institutions, and partner nations. The foundation is a surveillance system comprised of both active and passive monitoring of multiple environments and biomes—space, atmosphere, water, soil, animal reservoirs. Fundamental to the pandemic surveillance strategy is (i) training locals to conduct routine testing and genomic surveillance where spillovers occur and to regularly report incidences of novel illnesses, and (ii) increased genetic testing to track pathogens and to delineate what is coming from the natural environment versus being weaponized. Funding contributions and expert participation from other nations should be obtained.

Early detection would be enhanced by increasing the ability to identify and aggregate known data signals, identifying novel data signals, and enabling the combination of these signals into meaningful public health insights. This requires data to be labeled in such a way that it is globally recognized, named, and usable. Detection and monitoring also depend on developing distributed networks upon which those secured signals can arrive, inform local testing and response activities, and eventually be aggregated, while protecting personal data privacy, so that insights can be extracted. Finally, after preliminary flags or warning indicators are observed, a threshold is crossed and the warning or alarm could be sent throughout the distributed network, rather than relying upon a single entity or body to release the relevant information.

Key development principles include: (i) first determine a sufficient and obtainable set of data that the surveillance system should collect, and develop the local and regional capabilities to collect these data; (ii) support a global, decentralized network that can authenticate data sources, and enable validated data-sharing amongst validated data producers; (iii) enable cybersecure data aggregation and analysis capabilities while preserving personal data based on the terms specified in Recommendation 3.1 in this report; (iv) empower a surveillance strategy commensurate with civil liberties and privacy protections; (v) facilitate a surveillance strategy comprised of both active and passive monitoring of multiple environments and biomes (space, atmosphere, water, soil); (vi) facilitate a surveillance strategy comprised of monitoring of traditional health



and nontraditional data sources [e.g., excess death rates, viral genome sequences, Internet searches, geographic information systems (GIS), market trends]; and (vii) form distributed networks for global early warning system alerts.

**Recommendation 5.2: Reestablish and realign existing pandemic monitoring programs.**

The administration should provide R&D funding to current pandemic monitoring and response networks as part of the effort to build a system for continuous global health protection. The primary actions to consider include: reinstate the USAID PREDICT program<sup>173</sup> for tracking global zoonotic disease, provide additional funding to the EcoHealth Alliance,<sup>174</sup> and utilize networks to combine data being accumulated through parallel observation networks—e.g., the Strategic Advisory Group of Experts on Immunization (SAGE),<sup>175</sup> the National Ecological Observatory Network (NEON),<sup>176</sup> Collective and Augmented Intelligence Against COVID-19 (CAIAC),<sup>177</sup> and the Epidemic Intelligence from Open Sources (EIOS).<sup>178</sup>

**Recommendation 5.3: Emphasize privacy protections in pandemic surveillance systems.**

The administration should support initiatives that emphasize privacy protections in pandemic surveillance systems. These initiatives should be managed by NIST and NSF in collaboration with the Department of Health and Human Service's Office of the National Coordinator for Health Information Technology and the lead science institutions in partner nations. The mitigation strategies will (i) identify infected individuals early through robust and frequent testing with a globally-recommended strategy; (ii) deploy contact-tracing strategies (commensurate with civil liberties); (iii) deliver consistent health messaging for disease prevention, spread, and treatment by coordinating centralized information and data reporting with local, on-the-ground, trusted community leaders; and (iv) provide consistent public health guidance for gatherings like air travel, cruises, sporting events, schools, restaurants, stores, and so forth.

173 PREDICT, "Reducing Pandemic Risk, Promoting Global Health," USAID, <https://www.usaid.gov/sites/default/files/documents/1864/predict-global-flyer-508.pdf>.

174 "EcoHealth Alliance," website homepage accessed April 16, 2021, [https://www.who.int/groups/strategic-advisory-group-of-experts-on-immunization/working-groups/cholera-\(november-2015---august-2017\)](https://www.who.int/groups/strategic-advisory-group-of-experts-on-immunization/working-groups/cholera-(november-2015---august-2017)).

175 "Strategic Advisory Group of Experts on Immunization (SAGE)," World Health Organization, accessed April 16, 2021, [https://www.who.int/groups/strategic-advisory-group-of-experts-on-immunization/working-groups/cholera-\(november-2015---august-2017\)](https://www.who.int/groups/strategic-advisory-group-of-experts-on-immunization/working-groups/cholera-(november-2015---august-2017)).

176 "The National Science Foundation's National Ecological Observatory Network (NEON)," website homepage accessed April 16, 2021, <https://www.neonscience.org/>.

177 "CAIAC: Collective and Augmented Intelligence Against COVID-19," website homepage accessed April 16, 2021, <https://www.caiac19.org/>.

178 "Epidemic Intelligence from Open Sources (EIOS): Saving Lives through Early Detection," World Health Organization, <https://www.who.int/initiatives/eios>.

#### **Recommendation 5.4: Increase resilience in medical supply chains.**

The administration should fund R&D of cellular- and molecular-based manufacturing technologies<sup>179</sup> that enhance supply chain assurance.<sup>180</sup> Both cellular and molecular manufacturing are specific instances of synthetic biology. In some cases, they can be rapidly deployed by setting up the conditions for production, and then substituting in the genetic sequences of interest to go into high-gear production. This simplifies supply chain and production lead time, can increase capacity, and creates flexible supply chains by producing candidates that are thermostable.

Some of the more forward-looking technologies for bio-sensing, vaccine development, and therapeutics are amenable to this kind of manufacturing and stockpiling. The goal is to develop redundancy at a regional level (components/ingredients; manufacturing), adopt more rigorous methods for validation of authenticity, and support multiregional distribution chains.

#### **Recommendation 5.5: Develop capacity building for vaccine and therapeutics discovery, development, and distribution.**

The administration should establish PPPs to improve pandemic protection capacity building. There are three efforts: (i) biomanufacturing and synthetic biology innovations will create therapeutic discovery systems and speed vaccine discovery; (ii) vaccine discovery, development, and distribution coalitions like the Coalition for Epidemic Preparedness Innovations (CEPI) will enable equitable distribution; and (iii) information monitoring and distribution regarding consumables, capital equipment supplies, hospital resources, and healthcare workers will support public and organizational activities during a crisis.

#### **Recommendation 5.6: Develop rapid responses to unknown pathogens, and supporting data collection networks.**

NIH should develop and lead a program for the automated development of treatments for unknown pathogens. The goal is to universalize treatment methods; for example, by employing automated methods to massively select bacteriophages as a countermeasure to bacteria—or employ antibody-producing *E. coli* or cell-free synthetic biology as a countermeasure to viruses. Advanced computational methods such as computational

179 Megan Scudellari. "Step Aside, PCR: CRISPR-based COVID-19 Tests Are Coming." *IEEE Spectrum*, December 21, 2020, accessed April 16, 2021, <https://spectrum.ieee.org/the-human-os/biomedical/diagnostics/step-aside-pcr-crispr-based-covid-19-tests-are-coming>.

180 Nicholas A. C. Jackson et al., "The promise of mRNA vaccines: a biotech and industrial perspective," *npj Vaccines* 5 (11) (2020), <https://doi.org/10.1038/s41541-020-0159-8>, accessed March 26, 2021; Giulietta Maruggi et al., "mRNA as a Transformative Technology for Vaccine Development to Control Infectious Diseases," *Molecular Therapy* 27 (4) (April 10, 2019): 757–772, accessed March 26, 2021, <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6453507/>.

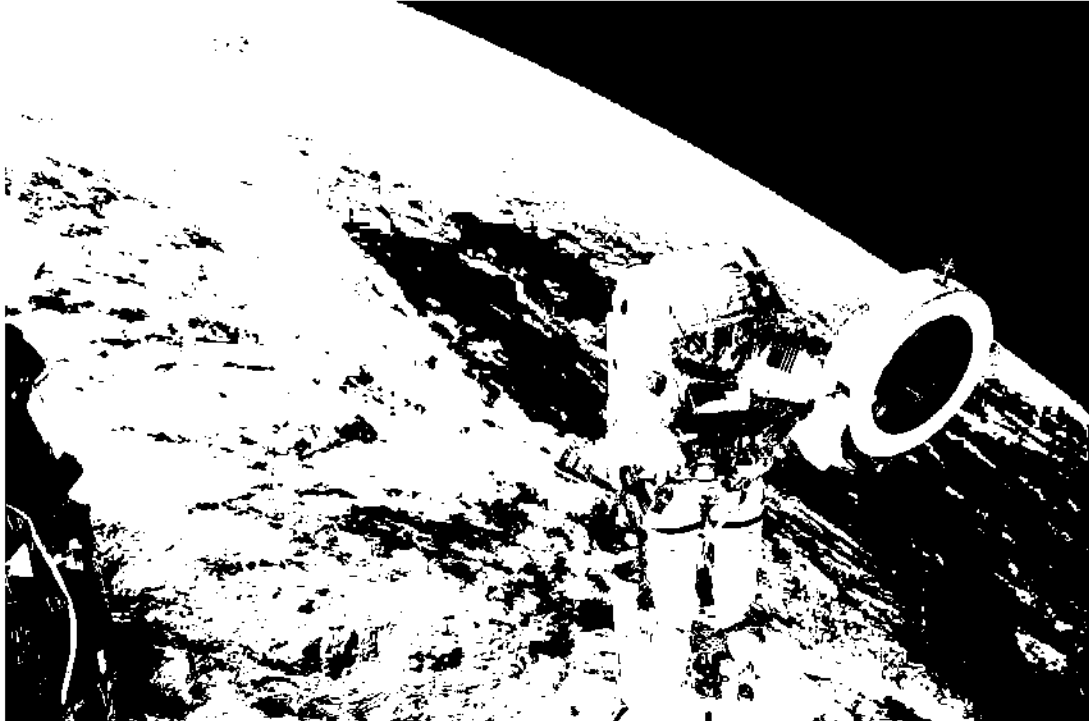
modeling of the 3D molecules of novel pathogens, and AI-based selection of potential treatments, can help automate and speed up this process. New technologies that can change the time for the regulatory approval process, i.e., the time required for human clinical trials, should be researched—for example, in silico testing or artificial organ testing.<sup>181</sup>

NIH should create a consortium of universities and biotechnology companies to develop rapid, wide-area distribution of vaccines. This program should consider approaches that distribute vaccines through conventional supply channels, and methods to make vaccines that are survivable and transportable in any environment. Treatments in addition to vaccines should be incorporated in this effort.

NSF should create a digital infrastructure that can connect diverse, independent observation networks, databases, and computers—including emerging biosensors and autonomous sequencers deployed in water systems, air filtration systems, and other public infrastructure—to integrate their diverse data for analysis and modeling with protocols for activating rapid analysis of new pathogens, including new strains of extant pathogens to evaluate ongoing vaccine efficacy.

181 Committee on Animal Models for Assessing Countermeasures to Bioterrorism Agents, Institute for Laboratory Animal Research Division on Earth and Life Studies, “Chapter 5: Alternative Approaches to Animal Testing for Biodefense Countermeasures,” in *Animal Models for Assessing Countermeasures to Bioterrorism Agents* (Washington, DC: The National Academies Press, 2011), accessed March 26, 2021, <https://www.nap.edu/read/13233/chapter/7>.

## Chapter 6. Assured Space Operations for Public Benefit



Astronaut Franklin R. Chang-Diaz works with a grapple fixture during extravehicular activity to perform work on the International Space Station

PHOTO BY NASA

**T**he growing commercial space industry enables ready access to advanced space capabilities for a broader group of actors. To maintain trusted, secure, and technically superior space operations, the United States must ensure it is a leading provider of needed space services and innovation in launch, on-board servicing, remote sensing, communications, and ground infrastructures. A robust commercial space industry not only enhances the resilience of the US national security space system by increasing space industrial base capacity, workforce, and responsiveness, but also further advances a dynamic innovative environment that can bolster US competitiveness across existing industries, while facilitating the development of new ones.

As smaller satellites become more capable, large constellations of government and commercial platforms could increase space mission assurance and deterrence by “eliminating mission critical, single-node vulnerabilities and distributing space operations

across hosts, orbits, spectrum, and geography.”<sup>182</sup> Advances in commercial space also enable exploring our planet’s oceans, monitoring for climate change-related risks, and mapping of other parts of our solar system.

The fast-growing critical dependence on space for national security, the global economy, and public-benefit interests makes assured space operations essential for ensuring a more free, secure, and prosperous world.

## **Finding 6: The US commercial space industry can increase its role in supporting national security.**

The National Space Strategy<sup>183</sup> includes four areas of emphasis: resilience, deterrence, foundational capabilities, and more conducive domestic and international environments. It envisions improved leverage of, and support for, the US commercial industry. The Defense Space *Strategy Summary*<sup>184</sup> highlights that the rapidly growing commercial space industry is introducing new capabilities as well as new threats to US space operations. A main effort in this strategy is to cooperate with industry and other actors to leverage their capabilities.

“Space Policy Directive-2—Streamlining Regulations on Commercial Use of Space,” provides support for the US commercial space industry.<sup>185</sup> In support of the overall policy of the executive branch to promote economic growth, protect national security, and encourage US leadership in space commerce, the directive requires reviews of the launch and reentry licensing for commercial space flight, the Land Remote Sensing Policy Act of 1992, the Department of Commerce’s organization of its regulation of commercial space flight activities, radio frequency spectrum, and export licensing regulations.<sup>186</sup>

The Government Accountability Office’s (GAO’s) report on the Department of Defense’s

182 John J. Klein, *The Influence of Commercial Space Capabilities on Deterrence*, Center for a New American Security, March 25, 2019, accessed March 26, 2021, <https://www.cnas.org/publications/reports/the-influence-of-commercial-space-capabilities-on-deterrence/>; US Deputy Secretary of Defense Robert Work’s speech to the Satellite Industries Association, March 7, 2016, accessed March 26, 2021, <https://www.defense.gov/Newsroom/Speeches/Speech/Article/696289/satellite-industries-association/>; Government Accountability Office, *Military Space Systems: DoD’s Use of Commercial Satellites to Host Defense Payloads Would Benefit from Centralizing Data*, July 2018, GAO-18-493, accessed March 26, 2021, <https://www.gao.gov/products/gao-18-493>.

183 White House, “An America First National Space Strategy,” accessed March 26, 2021, <https://aerospace.csis.org/wp-content/uploads/2018/09/Trump-National-Space-Strategy.pdf>.

184 Department of Defense, *Defense Space Strategy Summary*, June 2020, accessed March 26, 2021, [https://media.defense.gov/2020/Jun/17/2002317391/-1/-1/1/2020\\_DEFENSE\\_SPACE\\_STRATEGY\\_SUMMARY.PDF](https://media.defense.gov/2020/Jun/17/2002317391/-1/-1/1/2020_DEFENSE_SPACE_STRATEGY_SUMMARY.PDF).

185 Executive Office of the President, “Streamlining Regulations on Commercial Use of Space,” *Federal Register*, Space Policy Directive-2 of May 24, 2018, accessed March 26, 2021, <https://www.federalregister.gov/documents/2018/05/30/2018-11769/streamlining-regulations-on-commercial-use-of-space>.

186 Ibid.

(DoD's) use of commercial satellites<sup>187</sup> describes several potential benefits of including more responsive delivery of capabilities to space and increasing deterrence and resilience due to the larger number and distribution of commercial constellations of satellites.

**Finding 6.1: Large constellations of small satellites are being developed.**

The development of small satellites enables the proliferation of very large constellations of satellites. For example, several companies are currently planning constellations of communications satellites comprising an aggregate deployment of several thousand satellites in low Earth orbit (LEO). In total, the communications capacities could exceed tens of terabytes. This enables low-latency, high-bandwidth communications to any region, bringing valuable educational opportunities to underserved populations, and supporting new data-intensive communications in advanced countries.<sup>188</sup> Small Earth observation satellites are being deployed in constellations of hundreds of platforms by several companies. These can produce global coverage with revisit intervals ranging from minutes to hours. Several types of sensors are being deployed including electro-optical, synthetic aperture radar, and radio signal collection.<sup>189</sup> Companies in the United States, Europe, Russia, and China are actively pursuing these new capabilities.<sup>190</sup>

The ability to image any area, and to communicate with any area, will become commercially available to any individual, group, or government. Coupled with access to cloud computing and big data analytics, innovations will occur in many fields, e.g., precise, real-time weather and soil condition data for farmers to increase yield, ship tracking to aid logistics, indicators of disease spread to inform a pandemic observation network, and the like.

Large constellations may also contribute to deterrence. The larger number of platforms operating in conjunction with major military satellites may make the entire constellation more resilient.

The commercial space industry is developing satellite servicing capabilities. This helps extend the operating life of each satellite, though the ability to operate near another satellite is viewed negatively by adversaries.

**Finding 6.2: There is increasing focus on cybersecurity for commercial space systems.**

187 Government Accountability Office, *Military Space Systems*, 4.

188 Matthew A. Hallex and Travis S. Cottom, "Proliferated Commercial Satellite Constellations, Implications for National Security," *Joint Forces Quarterly* 97 (2nd Quarter 2020), accessed March 26, 2021, [https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-97/jfq-97\\_20-29\\_Hallex-Cottom.pdf?ver=2020-03-31-130614-940](https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-97/jfq-97_20-29_Hallex-Cottom.pdf?ver=2020-03-31-130614-940).

189 Ibid.

190 Ibid.

The “Space Policy Directive 5”<sup>191</sup> specifies the US policy for managing risks<sup>192</sup> to the growth and prosperity of its commercial space economy is to rely on “executive departments and agencies to foster practices within Government space operations and across the commercial space industry that protect space assets and their supporting infrastructure from cyber threats and ensure continuity of operations.” Several cybersecurity principles provide the foundation for these efforts, though the directive expects space system owners and operators to be responsible for implementing cybersecurity practices and does not address enforcement actions. No timeline for the development of regulations is provided.

**Finding 6.3: The UN Outer Space Treaty (OST) requires interpretation to determine when emerging commercial space platforms become targets.**

The growth in the commercial satellite industry will lead to lower-cost satellites with advanced sensors, communications, on-board computation, and security capability. Over time, each small satellite, when operated in large constellations, could be more useful for military purposes.

A key determinant in the application of the UN OST to the question of whether the military can use commercial satellites is “whether the commercial satellite is actively making a contribution to military action.”<sup>193</sup> For example, if the military is using a commercial communications satellite to relay its messages, the UN OST does not view the communications satellite as a military target. Full consideration of the treatment of dual-use commercial satellites is not settled and will evolve as more nations participate in the commercial space industry.<sup>194</sup> Yet, because nations like China and Russia already target (terrestrial) commercial networks as part of their computer network exploitation campaigns, it stands to reason that they will not necessarily recognize a distinction between commercial and military satellite targets.

191 White House, Memorandum on Space Policy Directive-5—Cybersecurity Principles for Space Systems, presidential memoranda, September 4, 2020, accessed March 26, 2021, <https://trumpwhitehouse.archives.gov/presidential-actions/memorandum-space-policy-directive-5-cybersecurity-principles-space-systems/>.

192 Office of the Director of National Intelligence, *Annual Threat Assessment of the US Intelligence Community*, April 9, 2021, accessed April 16, 2021, <https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf>; Todd Harrison, *Space Threat Assessment 2021*, Center for Strategic and International Studies, March 31, 2021, accessed April 16, 2021, <https://www.csis.org/analysis/space-threat-assessment-2021>.

193 “Practice Relating to Rule 10. Civilian Objects’ Loss of Protection from Attack,” ICRC IHL Database, Customary IHL, accessed March 26, 2021, [https://ihl-databases.icrc.org/customary-ihl/eng/docs/v2\\_rul\\_rule10](https://ihl-databases.icrc.org/customary-ihl/eng/docs/v2_rul_rule10).

194 P.J. Blount, “Targeting in Outer Space: Legal Aspects of Operational Military Actions in Space,” *Harvard National Security Journal Features*, accessed March 26, 2021, <https://harvardnsj.org/wp-content/uploads/sites/13/2012/11/Targeting-in-Outer-Space-Blount-Final.pdf>; Yun Zhao, *Space Commercialization and the Development of Space Law*, Oxford University Press, July 30, 2018, accessed March 26, 2021, <https://oxfordre.com/planetariyscience/view/10.1093/acrefore/9780190647926.001.0001/acrefore-9780190647926-e-42>.

**Finding 6.4: The development of constellations of small satellites beneficial to the military may require government support.**

Commercially viable capabilities in small satellites are advancing, but may not be sufficient for some military needs at this time. For example, the resolution of an electro-optical sensor for surveilling traffic is not useful for target identification, though it may be useful for tracking troop movements. A balanced policy would require the government to focus on the more exquisite capabilities that only it can provide, while relying on the commercial sector to meet other requirements. The government can also do more to send a signal to the markets that it supports these constellations and their capabilities by purchasing commercial data and services, thereby helping to ensure a strong commercial industrial base.

**Finding 6.5: Government support for commercial space activities can be strengthened.**

The growth of the commercial space industry occurring in several major countries<sup>195</sup> requires a review of US commercial space policy<sup>196</sup> as the roles of government and commercial industry change in key areas. The National Aeronautics and Space Administration (NASA) is establishing a wholly commercial capability to land humans on the moon (from lunar orbit), in contrast with the prior approach of government control of human space-flight.<sup>197</sup> There are efforts to consolidate and streamline the regulatory framework and organizations for US commercial space capabilities.<sup>198</sup> To support greater innovation and bolster US commercial space industries, recently proposed legislation identified ways to make the commercial space licensing process simpler, more timely, and more transparent.<sup>199</sup> These efforts attempt to balance commercial interests against the government's need to ensure the commercial space capabilities meet national security and foreign policy requirements. Such balancing may be less important as sensitive imagery becomes more available from foreign companies. To address urgent new requirements—e.g., on-orbit servicing of a space force, or continuous global observation in support of climate study, agriculture, and ocean systems—the government may require new policies to support increasing reliance on commercial space industries and new commercial space capabilities.

195 Congressional Research Service, *Commercial Space: Federal Regulation, Oversight, and Utilization*, updated November 29, 2018, accessed March 26, 2021, <https://fas.org/sgp/crs/space/R45416.pdf>.

196 American Space Commerce Free Enterprise Act of 2019, H.R. 2809 — 116th Congress (2019-2020), accessed March 26, 2021, <https://www.congress.gov/bill/115th-congress/house-bill/2809>.

197 Congressional Research Service, *Artemis: NASA's Program to Return Humans to the Moon*, updated January 8, 2021, accessed March 26, 2021, <https://fas.org/sgp/crs/space/IF11643.pdf>.

198 Jeff Foust, "Commerce Department seeks big funding boost for Office of Space Commerce," *SpaceNews*, February 16, 2020, accessed March 26, 2021, <https://spacenews.com/commerce-department-seeks-big-funding-boost-for-office-of-space-commerce/>.

199 In the 115th Congress (2017-2018), the American Space Commerce Free Enterprise Act (H.R. 2809) and the Space Frontier Act of 2018 (S. 3277) include provisions to streamline the licensing process.



**Approach 6: Accelerate the development and deployment of dual-use commercial satellites, including applications to Earth and space exploration.**

The United States should use the emerging commercial space industry, and large constellations of small satellites, to enhance the resilience of national security space missions. This will require a deliberate strategy to guide commercial system developments, and this must be balanced with benefits that accrue to the public. The United States should, with its allies, examine how to interpret current treaties when considering the new commercial space capabilities. The United States, its allies, and private industry should implement global Earth and space observation capabilities.

**Recommendation 6: Foster the development of commercial space technologies and develop a cross-agency strategy and approach to space that can enhance national security space operations and improve agriculture, ocean exploration, and climate change activities; align both civilian and military operations, and international treaties to support these uses.**

**Recommendation 6.1: Ensure federal investments in the commercial space industry deliver public benefits.**

Congress should pass legislation that directs the Office of Science and Technology Policy (OSTP) to lead an interagency initiative that develops an economic impact assessment of existing and future government investments in the US commercial space industry, as well as a public-private investment strategy for technology innovations and operating efficiencies that will ensure subsequent benefit to the public interest. Such benefits should contribute to global access to open data sets—via a space-based Internet, space-based cloud storage and computing—of Earth observation, global health, humanitarian applications, and other areas; it should also include suitable sharing of government-funded data collections among other government programs. A cross-agency group including the National Aeronautics and Space Administration (NASA), the National Geospatial-Intelligence Agency (NGA), the Defense Advanced Research Projects Agency (DARPA), relevant federal departments, private industry, and allied nations should develop the plans and partnerships for global Earth and space observation in support of environmental security.

**Recommendation 6.2: Foster commercial space technologies of strategic importance and protect these from foreign acquisition.**

Congress should direct a cross-agency group including NASA and the Department of Defense to conduct a joint review<sup>200</sup> of dual-use commercial space technologies and capabilities that are of strategic importance to national security space missions. The scope includes communications, on-orbit storage and computing, large constellations of small platforms, sensing, space situational awareness, satellite protection, launch, and on-orbit servicing. Congress should direct a streamlined licensing process and simplify regulations where appropriate. Such dual-use technologies should be reviewed for protection from foreign acquisition by the expanded authorities of the Committee on Foreign Investment in the United States (CFIUS)<sup>201</sup> and by the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence. The broadened role delineated by the Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA) enables CFIUS to review noncontrolling foreign investments in critical technologies and critical infrastructure in the US space industrial base. Congress should direct an assessment of how the FIRRMA reforms have been applied and the resulting effect.

**Recommendation 6.3: Harden the security of commercial space industry facilities and space assets.**

The administration should designate the commercial space industry as a critical infrastructure sector and develop a sector-specific plan for its protection. The Department of Commerce should be assigned as the Sector-Specific Agency and should work with international standards-setting groups to harden select commercial space capabilities, e.g., protect communications against cyber threats.

The cybersecurity of both military and commercial spacecraft is a growing concern. Threat actors are devoting more attention to attacking both the software/IT supply chain as well as vulnerabilities in the cyber defenses on spacecraft. Large commercial mega-constellations of small satellites are performing an increasing range of business and communications functions, yet do not necessarily conform to high cybersecurity standards. The US government does not have standards for the design of cyber-secure commercial satellites, though it is introducing self-certification programs for commercial satellite providers.

200 National Aeronautics and Space Administration, "Memorandum of Understanding Between the National Aeronautics and Space Administration and the United States Space Force," September 2020, [https://www.nasa.gov/sites/default/files/atoms/files/nasa\\_ussf\\_mou\\_21\\_sep\\_20.pdf](https://www.nasa.gov/sites/default/files/atoms/files/nasa_ussf_mou_21_sep_20.pdf). This does not address foreign acquisition of commercial space technologies of strategic importance.

201 Congressional Research Service, *The Committee on Foreign Investment in the United States (CFIUS)*, updated February 14, 2020, accessed March 26, 2021, <https://fas.org/sgp/crs/natsec/RL33388.pdf>.

The administration should extend the National Institute of Standards and Technology (NIST) cybersecurity maturity standards, guidelines, and best practices to the space domain, covering the space, link, ground, and user segments. The cyber-resilient design principles should consider the following: “Intrusion detection and prevention leveraging signatures and machine learning to detect and block cyber intrusions onboard spacecraft; a supply chain risk management (SCRM) program to protect against malware inserted in parts and modules; software assurance methods within the software supply chain to reduce the likelihood of cyber weaknesses in flight software and firmware; logging onboard the spacecraft to verify legitimate operations and aid in forensic investigations after anomalies; root-of-trust to protect software and firmware integrity; a tamper-proof means to restore the spacecraft to a known good cyber-safe mode; and lightweight cryptographic solutions for use in small satellites.”<sup>202</sup>

**Recommendation 6.4: Establish the conformance of emerging commercial space constellations to multinational agreements.**

The United States should lead a conference to assess future developments in the commercial space industry with respect to the UN OST, the Artemis Accords,<sup>203</sup> and other international agreements that may be constructed. The objective is to clarify the acceptable use of commercial space assets as these become of greater use in supporting militaries.

Commercial capabilities may, over time, provide essential portions of space-based surveillance, reconnaissance, communications, refueling, data storage and processing, and maintenance. As new military space capabilities become possible, there is an increased risk that these will be interpreted as “making an effective contribution to military action” and thereby become legitimate targets. These capabilities may include imaging satellites, communications satellites, space networks, satellite maintenance vehicles, launch vehicles, and so forth. A key area to clarify is the legal and technical assessment of what qualifies as “making an effective contribution to military action” involving space technology.<sup>204</sup>

202 Brandon Bailey et al., *Defending Spacecraft in the Cyber Domain*, Aerospace Corporation, November 2019, accessed March 26, 2021, [https://aerospace.org/sites/default/files/2019-11/Bailey\\_DefendingSpacecraft\\_11052019.pdf](https://aerospace.org/sites/default/files/2019-11/Bailey_DefendingSpacecraft_11052019.pdf).

203 National Aeronautics and Space Administration, *The Artemis Accords: Principles for Cooperation in the Civil Exploration and Use of the Moon, Mars, Comets, and Asteroids for Peaceful Purposes*, accessed March 26, 2021, <https://www.nasa.gov/specials/artemis-accords/img/Artemis-Accords-signed-13Oct2020.pdf>.

204 Dr. Cassandra Steer, *Why Outer Space Matters for National and International Security*, Center for Ethics and the Rule of Law, University of Pennsylvania, January 8, 2020, accessed March 26, 2021, <https://www.law.upenn.edu/live/files/10053-why-outer-space-matters-for-national-and>; Jackson Nyamuya Maogoto and Steven Freeland, “Space Weaponization and the United Nations Charter Regime on Force: A Thick Legal Fog or a Receding Mist?” *International Lawyer* 41 (4) (Winter 2007): 1091-1119, <http://www.jstor.org/stable/40707832>, accessed March 26, 2021, <https://www.law.upenn.edu/live/files/7860-maogoto-and-freeland-space-weaponizationpdf>; Blount, “Targeting”; Theresa Hitchens and Colin Clark, “Commercial Satellites: Will They Be Military Targets?” *Breaking Defense*, July 16, 2019, accessed March 26, 2021, <https://breakingdefense.com/2019/07/commercial-satellites-will-they-be-military-targets/>.

**Recommendation 6.5: Develop space technologies for mega-constellations of satellites that support monitoring the entire planet pervasively and persistently, at high resolution and communicate the information in near-real time.**

The administration should develop autonomous space operations technologies for large-scale constellations. This program, led by the DoD, NASA, and other elements of the national security space enterprise, would use AI technologies to minimize or eliminate human requirements for satellite control, information collection, and information analysis; and increase the speed of the information-to-decision loop.

The administration should encourage commercial space companies to develop cost-effective technologies that increase the survivability of commercial satellites as the operating regions become more crowded or contested. This may enable commercial satellites to operate in a greater variety of conditions, thereby providing expanded value to the United States.

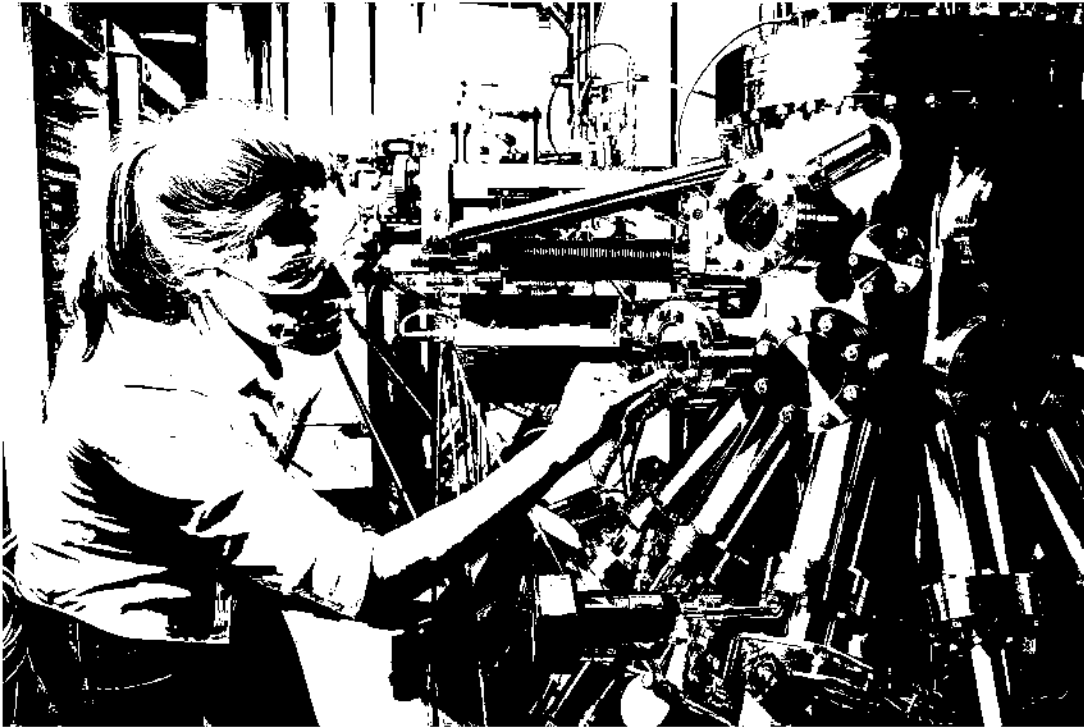
The administration should develop and conduct Challenge Prizes funding opportunities for autonomous satellite operations on single platforms, i.e., for applications where highly capable satellites autonomously manage their own complex taskings, and also work as part of a large collection of similarly autonomous satellites.

The administration should use the model of the NASA Tipping Point solicitation to develop the capability to continuously monitor the world's oceans—in particular, using space-based sensors—for the impact of climate change and other issues of global importance. This program would be jointly managed by NASA, NSF, and DARPA with collaborations from the European Union (EU) and other participants. This multiyear initiative would help establish a global, real-time Earth oceans observation network and the supporting autonomous control, communications, and data analytics capabilities. In addition to space technologies, this program could also support the development of surface and underwater vehicles to perform this function. The Department of State should address the treaty implications of large numbers of remotely-piloted and autonomous surface and underwater vehicles and develop new international agreements where needed.



## Chapter 7. Future of Work

---



A scientist at the National Renewable Energy Laboratory in Colorado uses a semiconductor growing system at the Solar Energy Research Facility.

PHOTO BY AP/WIDEWORLD

**W**hile this report has focused on the technological changes that will impact geopolitics over the next decade, the recommendations contained within will be meaningless if the United States and allied nations ignore the most important ingredient in the success or failure of all endeavors: people. Developing a digitally fluent and resilient workforce that can meet the challenges of the GeoTech Decade will require private and public sectors to pursue several approaches. These include a broadened view of technical competencies and how they are acquired, improved alignment of skills and job requirements, incentives for employer-based training, and data collection to help assess the effectiveness of these investments and their effects on workers. Ensuring that people, especially people from underrepresented communities, are not left behind by the advance of technology—and that societies have the skilled workforces they need to innovate and prosper—will determine whether the GeoTech Decade lives up to its ambition.

From artificial intelligence (AI) to quantum computing, and for applications ranging from augmented reality to smart cities and communities,<sup>205</sup> the technologies that will shape

205 Smart Cities and Communities Act of 2019, H.R. 2636 — 116th Congress (2019-2020), accessed March 26, 2021, <https://www.congress.gov/116/bills/hr2636/BILLS-116hr2636ih.pdf>.

the GeoTech Decade require specialized investments in the US workforce.<sup>206</sup> Shifting from the “findings and recommendations” format of the previous chapters, this closing chapter discusses key areas needing greater focus and investment from businesses, governments, educational institutions, and stakeholder organizations, as follows.

## **Create the Workforce for the GeoTech Decade**

### **Recognize the diverse competencies that characterize skilled technical workers**

Diverse competencies include academic credentials, technical competencies in an industry, and technical competencies in a specific occupation, plus “soft skills” that make for reliable and collegial employees.<sup>207</sup> Job descriptions should consider the value of all sources of relevant experience and ability.

### **Communicate the breadth of pathways for gaining skilled technical work**

Given the current focus on a college degree being a prerequisite to desirable, skilled technical jobs, the workforce should be better informed about the variety of skilled technical occupations, the different ways of acquiring credentials, e.g., college certificates, professional certifications, professional licenses, and digital badges and how such credentials allow more points of entry into desired occupations.

### **Strengthen skilled technical training and education**

Secondary school: Career and technical education (CTE) programs<sup>208</sup> enable the acquisition of STEM education combined with work experience that teaches technical skills relevant to specific professions. CTE programs can be enhanced through active participation and guidance provided by representatives from local businesses. This could help ensure that the skills training is better matched with employer needs and requirements. The P-TECH program, now operating schools in eleven US states, Australia, Morocco, and Taiwan, is another model for building regional workforces with the needed technical skills and for providing underserved youths with opportunities for gaining relevant technical skills.<sup>209</sup>

206 National Academies of Sciences, Engineering, and Medicine, *Building America's Skilled Technical Workforce* (Washington, DC: National Academies Press, 2017) accessed April 16, 2021, <http://nap.edu/23472>; Mark Warner, “Part II. Investing in Workers,” Medium, February 8, 2021, accessed April 16, 2021, <https://senmarkwarner.medium.com/ii-investing-in-workers-e7e9a09ff24c>.

207 National Academies of Sciences, Engineering, and Medicine, *Building America's Skilled*.

208 Bri Stauffer, “What Is Career & Technical Education (CTE)?” Applied Educational Systems, February 4, 2020, accessed April 16, 2021, <https://www.aeseducation.com/blog/career-technical-education-cte>.

209 “What is P-TECH all about?” website homepage accessed April 16, 2021, <https://www.ptech.org/>.

Post-secondary school: There are 936 public community colleges in the United States,<sup>210</sup> representing a nationwide resource for improving the technical skills of the current and future workforce. According to a Community College Resource Center analysis, “6.7 million students were enrolled at community colleges in fall 2017, and nearly 10 million students enrolled at a community college at some point during the 2017-18 academic year. Yet, the overall percent of community college enrollees in 2014 that completed a college degree at a four-year institution within six years is 17 percent.”<sup>211</sup> Increasing this completion rate through financial incentives and investments could increase the number and qualifications of the technically skilled workforce in the United States.

Non-college credentials: The value to the worker and the employer of non-college degree certification programs—apprenticeships, certifications, certificate programs—could be improved by better linking them to established, defined technical workforce competencies. Improved standards and data on the effectiveness of these credentials will help workers and employers determine the value of these credentials and enable more informed choices for skills training.

Alternative sources of skilled workers: A recent study<sup>212</sup> examined the prevailing practice of a four-year college degree being a prerequisite for skilled jobs. The analysis identified large populations of workers with suitable skills but who did not have a college degree. Of these, the analysis showed that twenty-nine million have skills that would enable them to transition to an occupation with a significantly higher wage. These results suggest that job descriptions should be carefully specified so as to reach the largest qualified talent pool.

### **Better align employer-based training with needs**

Business incentives: Incentives for employers to invest in improving workforce technical skills should help a company remain competitive. The investments would align the employer’s needs for technically skilled workers and the training and education that is offered. One approach could be based on tax incentives for increasing investment in workforce skill development to increase productivity.”<sup>213</sup>

210 “Number of community colleges in the United States in 2021, by type,” Statista, accessed April 16, 2021, <https://www.statista.com/statistics/421266/community-colleges-in-the-us/>.

211 “Community College FAQs,” Community College Research Center, Teachers College, Columbia University, accessed April 16, 2021, <https://ccrc.tc.columbia.edu/Community-College-FAQs.html>.

212 Peter Q. Blair et al., “Searching for STARS: Work Experience as a Job Market Signal for Workers without Bachelor’s Degrees,” National Bureau of Economic Research, March 2020, accessed April 16, 2021, <https://www.nber.org/papers/w26844>.

213 Warner, “Part II. Investing in Workers.”



**Technology development and training:** Workforce organizations can play a role in effectively communicating, between employers and the workforce, issues concerning needed technical skills and the mechanisms and policies being used to manage these requirements. To accelerate identifying and acquiring future technical skills needed by the workforce, technology development programs could also create a training program for the skills associated with using the new technology in a product. This can shorten the link between technology development and the training of workers.

### **Acquire and analyze human capital development and management data**

Human capital development and management data should address projections of the supply and demand for workers according to categories of technical skills, results of the search and hiring process, and how well the employer's needs were satisfied. The data also should inform how well the training policies provided equitable access to skills training across the workforce.

These data should enable analyses of the expected value of different options for skills education and training for workers, the return on the investment of workforce training for businesses, and options for adjusting workforce training policies.

### **Foster lifelong learning**

The pace at which advanced technology is changing the workplace and the skills needed to maintain a competitive economy makes lifelong learning imperative. Individuals should be able to guide their training and education throughout their working years.

To accomplish this on a national scale will require effort to craft incentives that motivate individuals to embrace this approach. Important elements may involve information on the value of continuing educational programs and the job opportunities that are enabled, funding mechanisms to lower the cost to the individual, and strategies developed with businesses that specify how continuing learning enhances an individual's work prospects.

To guide individual choices, new tools can facilitate gathering and synthesizing the complex array of information on skills, occupations, training opportunities, and assessments of their value. The tools can also help the individual identify and secure funding from available sources, and help government funding sources be applied efficiently to this long-term challenge.

## **Equitable Access to Opportunity**

The United States needs to ensure equitable access to opportunity during the GeoTech Decade. From access to affordable broadband to digital literacy, governments and the private sector need to make significant investments and work together to reduce barriers to full participation in the economy.

### **Access to affordable, high-speed Internet and devices to use it**

Ensuring that all people can participate in the GeoTech Decade requires a commitment to equitable access to affordable, high-speed Internet. Millions do not have high-speed broadband, particularly in rural areas.<sup>214</sup> What is more, many with access to high-speed broadband are still unable to afford the high cost of Internet and the devices needed to access it.<sup>215</sup> Lack of access and affordability perpetuates systemic inequities.

While Congress has made significant investments in broadband since the onset of the COVID-19 pandemic, more remains to be done. The Emergency Broadband Benefit Program has helped low-income households afford broadband during the pandemic.

### **Acquiring digital literacy**

Digital literacy, the ability to find, evaluate, utilize, and create information using digital technology, is becoming an essential skill for every individual. Digital literacy is an important element in eliminating a digital divide among nations and within a society. It complements affordable, high-speed Internet access by enabling people to develop and communicate local content, to communicate their issues and concerns, and to help others understand the context in which these issues occur.

214 Federal Communications Commission, *2020 Broadband Deployment Report*, April 24, 2020, accessed April 16, 2021, <https://docs.fcc.gov/public/attachments/FCC-20-50A1.pdf>.

215 Tom Wheeler, *5 steps to get the internet to all Americans COVID-19 and the importance of universal broadband*, Brookings Institution, May 27, 2020, accessed April 16, 2021, <https://www.brookings.edu/research/5-steps-to-get-the-internet-to-all-americans/>.



# Conclusion

---

**T**he increasing capabilities and availability of data and new technologies change how nations remain competitive and secure. In the coming GeoTech Decade, data and technology will have a disproportionate impact on geopolitics, global competition, and global opportunities for collaboration as new capabilities may eliminate a technical advantage or may enable new processes superior to current methods. The United States and like-minded nations must be able to adapt and demonstrate effective governance, at faster speeds, in employing data and new technologies to promote a more secure, free, and prosperous world.

In 1945, Vannevar Bush, director of the Office of Scientific Research and Development, transmitted a report, *Science – the Endless Frontier*,<sup>216</sup> with the goal of answering a few key questions asked by then-President Franklin D. Roosevelt in November 1944. In the report, Bush elaborated:

“With particular reference to the war of science against disease, what can be done now to organize a program for continuing in the future the work which has been done in medicine and related sciences?”

“What can the Government do now and in the future to aid research activities by public and private organizations?”

“Can an effective program be proposed for discovering and developing scientific talent in American youth so that the continuing future of scientific research in this country may be assured on a level comparable to what has been done during the war?”

Among its recommendations, the 1945 report called for the creation of the National Research Foundation. Bush concluded, noting the importance of action by Congress:

“Legislation is necessary. It should be drafted with great care. Early action is imperative, however, if this nation is to meet the challenge of science and fully utilize the potentialities of science. On the wisdom with which we bring science to bear against the problems of the coming years depends in large measure our future as a nation.”

Now, almost seventy-six years later, the GeoTech Commission similarly seeks to promote freedom and security through initiatives that employ data and new technologies to amplify the ingenuity of people, diversity of talent, strength of democratic

216 *Science – The Endless Frontier*, a report to the president by Vannevar Bush, director of the Office of Scientific Research and Development, July 1945, accessed March 26, 2021, <https://nsf.gov/od/lpa/nsf50/vbush1945.htm>.

values, innovation of companies, and the reach of global partnerships.

There are several areas where data and technology can help, or hinder, the achievement of these goals:

- Communications and networking, data science, cloud computing
- Artificial intelligence, distributed sensors, edge computing, the Internet of Things
- Biotechnologies, precision medicine, genomic technologies
- Space technologies, undersea technologies
- Autonomous systems, robotics, decentralized energy methods
- Quantum information science, nanotechnology, new materials for extreme environments, advanced microelectronics

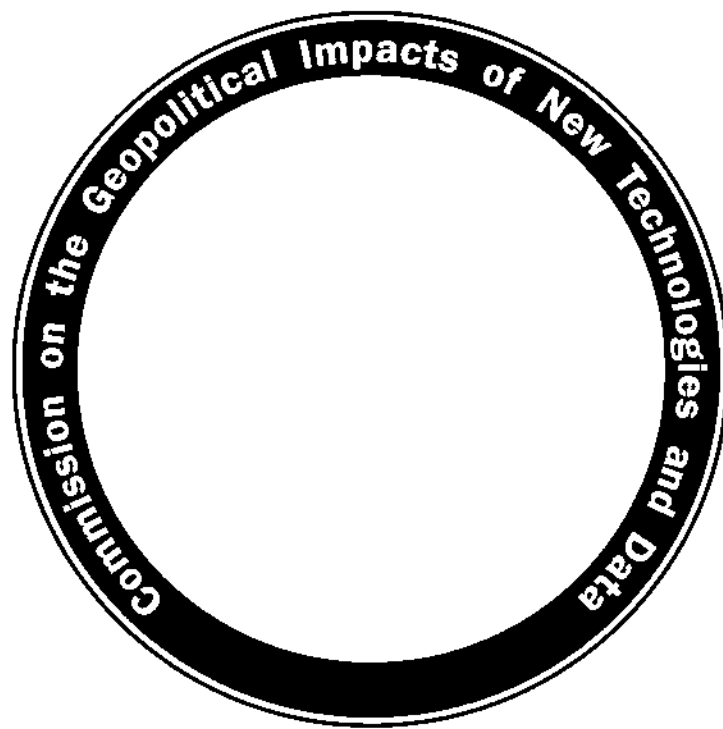
To maintain national and economic security and competitiveness in the global economy, the United States and its allies must continue to be preeminent in these key areas, and must achieve trustworthy and assured performance of the digital economy and its infrastructure. The GeoTech Commission provided recommendations in the following seven areas where the United States and like-minded nations must succeed:

- **Global science and technology leadership**
- **Secure data and communications**
- **Enhanced trust and confidence in the digital economy**
- **Assured supply chains and system resiliency**
- **Continuous global health protection and global wellness**
- **Assured space operations for public benefit**
- **Future of work**

The report's recommendations embody several ideals. First, work to ensure the benefits of new technologies reach all sectors of society. Second, define protocols and standards for permissible ways to develop and use technologies and data, consistent with the norms of the United States and like-minded nations. Third, guide technology cooperation and sharing with nondemocratic nations based on respecting democratic values.

Just as Vannevar Bush urged in 1945, the United States must create new ways to develop and employ future critical and emerging technologies at speed, cultivate the needed human capital, and establish norms for international cooperation with nations. Such creation requires important action by Congress and the new administration to

ensure that the United States has the wisdom with which to apply science to the challenges and opportunities of the coming years. If enacted, the report's recommendations will enable the United States and like-minded nations to employ data capabilities and new technologies intentionally to promote a freer, more secure, and more prosperous world.



# Appendix A. Additional Readings on Identifying and Countering Online Misinformation

Misinformation has existed for most of human history and has been wielded to influence geopolitics. Johns Hopkins University's Sheridan Libraries defines misinformation as follows:

"‘Misinformation’ is defined as the action of misinforming or the condition of being misinformed; or erroneous or incorrect information. Misinformation differs from propaganda in that it always refers to something which is not true. It differs from disinformation in that it is ‘intention neutral’; that is, misinformation is not deliberate, just wrong or mistaken. One of the most popular forms of misinformation on the Internet is the passing along of ‘urban legends.’ Urban legends are fabricated or untrue stories that are passed along by sincere people who believe them, and then ‘inform’ others."<sup>217</sup>

Recent advances with the Internet and social media have provided a way to propagate misinformation and disinformation more rapidly and democratized the ability for both individuals and automated programs ("bots") to accelerate their propagation online. As digital technologies have become democratized, so too has the ability for others to use these technologies to shape narratives in ways that were not readily available thirty or forty years ago. As we navigate the GeoTech Decade ahead, we will need to identify solutions to sift through all the information produced and shared online. Listing in chronological order from 2015 to 2021, these five readings represent scholarly research on this evolving topic area.

217 "Evaluating Information: Information and Its Counterfeits: Propaganda, Misinformation and Disinformation," Sheridan Libraries, Johns Hopkins, <https://guides.library.jhu.edu/evaluate/propaganda-vs-misinformation>.

## **1. This Is Why We Can't Have Nice Things: Mapping the Relationship between Online Trolling and Mainstream Culture**

Author: Whitney Philips

Publication date: 2015

Publisher: MIT Press

Excerpt from the publication:

"Trolls also fit very comfortably within the contemporary, hyper-networked digital media landscape. Not only do they put internet technologies to expert and highly creative use, their behaviors are often in direct (if surprising) alignment with social media marketers and other corporate interests. Furthermore, they are quite skilled at navigating and in fact harnessing the energies created when politics, history, and digital media collide. In short, rather than functioning as a counterpoint to 'correct' online behavior, trolls are in many ways the grimacing poster children for the socially networked world."

Link: <https://www.jstor.org/stable/j.ctt17kk8k7>

## **2. Media Manipulation and Disinformation Online**

Authors: Alice Marwick and Rebecca Lewis

Publication date: May 15, 2017

Publisher: Data & Society Research Institute

Excerpt from the report:

"'Trolling' developed in tandem with the internet. Initially, the term 'troll' described those who deliberately baited people to elicit an emotional response. Early trolls posted inflammatory messages on Usenet groups in an attempt to catch newbies in well-worn arguments. During the '00s, this motivation became known as the 'lulz': finding humor (or LOLs) in sowing discord and causing reactions. Trolls have a history of manipulating the media to call out hypocrisies and hysterias, learning early on how to target public figures and organizations to amplify their efforts through mainstream media. They have often claimed to be apolitical and explained their use of shocking (often racist or sexist) imagery as merely a convenient tool to offend others. Trolling can refer to relatively innocuous pranks, but it can also take the form of more serious behaviors. Trolling can include 'mischievous activities where the intent is not necessarily to cause distress' or it can seek to 'ruin the reputation of individuals and organizations and reveal embarrassing or personal information.' In practice, however, trolling has grown to serve as an umbrella term which encompasses a wide variety of asocial internet behaviors."

Link: [https://www.datasociety.net/pubs/oh/DataAndSociety\\_MediaManipulationAndDisinformationOnline.pdf](https://www.datasociety.net/pubs/oh/DataAndSociety_MediaManipulationAndDisinformationOnline.pdf)



### 3. Source Hacking: Media Manipulation in Practice

Authors: Joan Donovan and Brian Friedberg

Publication date: September 4, 2019

Publisher: Data & Society Research Institute

Excerpt from the report:

“In recent years there has been an increasing number of online manipulation campaigns targeted at news media. This report focuses on a subset of manipulation campaigns that rely on a strategy we call source hacking: a set of techniques for hiding the sources of problematic information in order to permit its circulation in mainstream media. Source hacking is therefore an indirect method for targeting journalists—planting false information in places that journalists are likely to encounter it or where it will be taken up by other intermediaries.

“Across eight case studies, we identify the underlying techniques of source hacking to provide journalists, news organizations, platform companies, and others with a new vocabulary for describing these tactics, so that terms such as ‘trolling’ and ‘trending’ do not stand in for concerted efforts to pollute the information environment. In this report, we identify four specific techniques of source hacking:

- Viral Sloganeering: repackaging reactionary talking points for social media and press amplification
- Leak Forgery: prompting a media spectacle by sharing forged documents
- Evidence Collages: compiling information from multiple sources into a single, shareable document, usually as an image
- Keyword Squatting: the strategic domination of keywords and sockpuppet accounts to misrepresent groups or individuals

“These four tactics of source hacking work because networked communication is vulnerable to many different styles of attack and finding proof of coordination is not easy to detect. Source hacking techniques complement each other and are often used simultaneously during active manipulation campaigns. These techniques may be carefully coordinated but often rely on partisan support and buy-in from audiences, influencers, and journalists alike.”

Link: <https://apo.org.au/node/257046>

#### **4. Deepfakes and Cheap Fakes: The Manipulation of Audio and Visual Evidence**

Authors: Britt Paris and Joan Donovan

Publication date: September 18, 2019

Publisher: Data & Society Research Institute

Excerpt from the publication:

“The first widely-known examples of amateur, AI-manipulated, face swap videos appeared in November 2017. Since then, the news media, and therefore the general public, have begun to use the term ‘deepfakes’ to refer to this larger genre of videos—videos that use some form of deep or machine learning to hybridize or generate human bodies and faces. News coverage claims that deep-fakes are poised to assault commonly-held standards of evidence, that they are the harbingers of a coming ‘information apocalypse.’ But what coverage of this deepfake phenomenon often misses is that the ‘truth’ of audiovisual content has never been stable—truth is socially, politically, and culturally determined.

“Deepfakes which rely on experimental machine learning represent one end of a spectrum of audio-visual (AV) manipulation. The deepfake process is both the most computationally-reliant and also the least publicly accessible means of creating deceptive media. Other forms of AV manipulation –‘cheap fakes’ –rely on cheap, accessible software, or no software at all. Both deepfakes and cheap fakes are capable of blurring the line between expression and evidence. Both can be used to influence the politics of evidence: how evidence changes and is changed by its existence in cultural, social, and political structures.”

Link: [https://datasociety.net/wp-content/uploads/2019/09/DS\\_Deepfakes\\_Cheap\\_FakesFinal-I-1.pdf](https://datasociety.net/wp-content/uploads/2019/09/DS_Deepfakes_Cheap_FakesFinal-I-1.pdf)

## 5. ‘Stop the Presses? Moving from Strategic Silence to Strategic Amplification in a Networked Media Ecosystem’

Authors: Joan Donovan and Danah Boyd

Publication date: September 29, 2019

Publisher: *American Behavioral Scientist* (65) (2): 333–350, SAGE Publications

Excerpt from the publication:

“In a media ecosystem besieged with misinformation and polarizing rhetoric, what the news media chooses not to cover can be as significant as what they do cover. In this article, we examine the historical production of silence in journalism to better understand the role amplification plays in the editorial and content moderation practices of current news media and social media platforms. Through the lens of strategic silence (i.e., the use of editorial discretion for the public good), we examine two U.S.-based case studies where media coverage produces public harms if not handled strategically: White violence and suicide. We analyze the history of journalistic choices to illustrate how professional and ethical codes for best practices played a key role in producing a more responsible field of journalism. As news media turned to online distribution, much has changed for better and worse. Platform companies now curate news media alongside user generated content; these corporations are largely responsible for content moderation on an enormous scale. The transformation of gatekeepers has led an evolution in disinformation and misinformation, where the creation and distribution of false and hateful content, as well as the mistrust of social institutions, have become significant public issues. Yet it is not just the lack of editorial standards and ethical codes within and across platforms that pose a challenge for stabilizing media ecosystems; the manipulation of search engines and recommendation algorithms also compromises the ability for lay publics to ascertain the veracity of claims to truth. Drawing on the history of strategic silence, we argue for a new editorial approach—‘strategic amplification’—which requires both news media organizations and platform companies to develop and employ best practices for ensuring responsibility and accountability when producing news content and the algorithmic systems that help spread it.”

Link: <https://journals.sagepub.com/doi/abs/10.1177/0002764219878229>

# Appendix B. Improving the Software Supply Chains and System Resiliency for the US Government

## Overview

Since FireEye's public disclosure<sup>218</sup> on December 8, 2020, of the theft of its penetration testing toolkit, story after story has revealed the staggering breadth of a comprehensive cyber breach centered on SolarWinds' Orion network monitoring software. State-sponsored adversaries compromised the widely used program in its build stages, allowing them to infiltrate over eighteen thousand commercial and government targets, including Intel, Microsoft, California state hospitals,<sup>219</sup> the National Nuclear Security Administration,<sup>220</sup> and dozens<sup>221</sup> of federal, state, and local government agencies, reportedly with the goal of extracting valuable intelligence.

The SUNBURST event<sup>222</sup> is a case study in software supply chain attacks, in which attackers compromise targets by exploiting vulnerabilities not just within target networks and infrastructure themselves, but in the programs and code that those systems rely on, either through programmed dependency or purchase and acquisition. Attackers are migrating<sup>223</sup> toward the most vulnerable points in complex digital supply chains, employing attacks resembling the SUNBURST event: compromised updates and installers used as distribution networks to create entry points into sensitive systems,

218 Kevin Mandia, "FireEye Shares Details of Recent Cyber Attack, Actions to Protect Community," FireEye, December 08, 2020, accessed March 26, 2021, <https://www.fireeye.com/blog/products-and-services/2020/12/fireeye-shares-details-of-recent-cyber-attack-actions-to-protect-community.html>.

219 Hautala, "SolarWinds hackers accessed DHS acting secretary's emails."

220 Bertrand and Wolff, "Nuclear weapons agency."

221 Satter, "U.S. cyber agency."

222 SolarWinds' Orion program was not the only vector pursued by attackers. However, it has received the most public scrutiny so far and is the purest supply chain component of the attack. As such, the expansive intelligence gathering operation is, throughout this appendix, referred to as the SUNBURST campaign, to acknowledge the central role of the most notorious piece of associated malware, with full acknowledgement that the nomenclature oversimplifies an extraordinarily sophisticated event involving many vectors, which were not always related.

223 Sonatype, 2020 State of the Software Supply Chain Report, accessed March 26, 2021, <https://www.sonatype.com/campaign/wp-2020-state-of-the-software-supply-chain-report>.

perpetrated by state-backed attackers with deeply sophisticated methods. Data from the Atlantic Council's Breaking Trust report<sup>224</sup> found thirty-six attacks in recent years bearing similar characteristics. Attackers pick at the weak points on software supply chains and pose a critical threat to national security; government procedures, born out of traditional processes designed for the acquisition of physical systems,<sup>225</sup> are ill-suited to moderate the dynamic and complex software ecosystem.

The software supply chain provides remarkable return on investment for attackers, where successfully undermining one update or installer can provide attackers access to thousands of systems and millions of machines. The software supply chains are increasingly leveraged in a cyber espionage contest. State-backed actors work to compromise widely used and deeply permissioned software to seek useful intelligence and intellectual property. In this realm, deterrence is difficult, capabilities wide-ranging, and precise, public attribution of the most successful breaches challenging, both technically and, sometimes more importantly, politically. It is not simply a story of compromised products but also the insecure configurations within vulnerable networks backed by limited staff resources and burdened by immense complexity and rapid change. The problem as manifested in federal acquisition practices is not primarily technological or geopolitical, but organizational. Such attacks may further erode the United States' competitive edge and compromise its national security.

This appendix focuses on the main lines of effort that the US government must undertake to improve the security of software supply chains, informed by its current shortcomings: improving baseline requirements, empowering agencies to implement basic supply chain risk management (SCRM) practices, reframing software security as a holistic undertaking, better coordinating between agencies and network types, and improving private sector involvement. This appendix focuses specifically on government acquisition processes and certification policies, addressing direct national security concerns. It does not recommend specific legislation but rather the end states towards which any reforms must strive.

224 Trey Herr et al., "Breaking trust: The Dataset," Cyber Statecraft Initiative, Atlantic Council, accessed March 26, 2021, <https://www.atlanticcouncil.org/resources/breaking-trust-the-dataset/>.

225 J. Michael McQuade et al., *Software Is Never Done: Refactoring the Acquisition Code for Competitive Advantage*, Defense Innovation Board, May 3, 2019, accessed March 26, 2021, <https://media.defense.gov/2019/May/01/2002126689/-1/-1/0/SWAP%20COMPLETE%20REPORT.PDF>.

## Lines of Improvement

**Meet the Baselines:** The December 2020 Government Accountability Office (GAO) report, *Federal Agencies Need to Take Urgent Action to Manage Supply Chain Risks*,<sup>226</sup> on software/IT supply chain risk management (SCRM) implementation found that, of twenty-three studied federal civilian agencies, no agency had implemented the seven foundational practices. Fourteen had not implemented any. Most agencies cited either insufficient guidance, inadequate bandwidth and staff power, or the overwhelming burden of implementation. Some delegated the task to internal bureaus and initiatives, while others preferred to deal with software/IT supply chain challenges as they came. The systemic failure to comply with “Office of Management and Budget (OMB) Circular No. A-130, Managing Information as a Strategic Resource,” the main directive examined by the GAO report, indicates a clear need for centralized assistance to prioritize and address the known shortcomings of federal agencies’ software/IT supply chain practices. Such an effort must balance helping agencies establish and formalize their SCRM practices with leveraging their knowledge of their own networks and practices.

**Mature the Baselines:** The many federal guidance documents on software SCRM—OMB Circular A-130, the Department of Defense’s (DoD’s) new *Cybersecurity Maturity Model Certification (CMMC)*, the Federal Information Security Modernization Act (FISMA), the DoD Information Network (DoDIN) Approved Products List (APL), the Federal Risk and Authorization Management Program (FedRAMP), and more—all draw on a common set of security guidelines laid out by the National Institute of Standards and Technology (NIST), mainly in Special Publications 800-53 for agencies and 800-171 for vendors managing Controlled Unclassified Information (CUI), as well as several other 800 series publications. These guidelines apply to the agencies assuming the risk of acquired products, the vendors providing them, and the products themselves. The NIST Cybersecurity Framework, far from providing specific recommendations, is more akin to a static checklist of best practices in thinking about cybersecurity. For example, SolarWinds’ Orion program was on DoDIN’s APL,<sup>227</sup> was Common Criteria certified,<sup>228</sup> had Federal Information Processing Standards (FIPS) 140-2 compliant modules and modes,<sup>229</sup> and so on. The standards were insufficient to protect against an extremely sophisticated threat. More concrete, verifiable vendor practices and product

226 Government Accountability Office, *Information Technology: Federal Agencies Need*.

227 “DoDIN Approved Products List,” DISA, accessed March 26, 2021, <https://aplits.disa.mil/processAPList.action>.

228 “SolarWinds Orion Suite v3.0 Added to DoDIN APL,” SolarWinds, accessed March 26, 2021, <https://www.solarwinds.com/federal-government/solution/dodin-apl>; technically they are certified. However, they were only certified to Evaluation Assurance Level AL 2+ which is low; the highest level is 7. EAL 2+ is insufficient to trust a product with administrative credentials to the network.

229 “Documentation for Orion Platform: Enable FIPS for Orion Platform products,” SolarWinds, accessed March 26, 2021, [https://documentation.solarwinds.com/en/Success\\_Center/orionplatform/content/core-enabling-fips-sw1508.htm](https://documentation.solarwinds.com/en/Success_Center/orionplatform/content/core-enabling-fips-sw1508.htm).

characteristics are necessary, and such predictability will also ease the burden of compliance on vendors.

- **Assume Compromise and Mitigate:** Even the most rigorous checks will fail to prevent every incursion, especially by the most capable, state-backed threat actors. With the assumption that breach is inevitable, it is crucial that agency practices mitigate the spread of breaches and impose costs on attackers. Post-compromise lateral movement was a significant part of the SUNBURST incident, leveraging vulnerabilities in Security Assertion Markup Language (SAML) tokens<sup>230</sup> and Azure Active Directory configurations. Agencies, where possible, must implement best network practices such as least privileged access, whitelisting, and authentication auditing to reduce the blast radius of compromised software.
- **Monitor Compliance Continuously:** While NIST 800-53 and 800-171 provide some guidance on the systems-level continuous monitoring of security controls within vendors and agencies (with more in-depth discussions in NIST 800-137), most acquisition systems are still based on periodic review over a long time frame. FISMA compliance is reviewed annually,<sup>231</sup> CMMC incorporates annual reviews<sup>232</sup> and is generally valid for three years, FedRAMP<sup>233</sup> incorporates both annual assessments and monthly reports, and DoDIN APL<sup>234</sup> listing is valid for three years with the option to extend by another three. Such periodicity, even if supplemented with review of patches and ongoing assessment, is out of step with the rapid dynamism of software development, and where possible, agencies should implement and automate compliance monitoring continuously. The aforementioned programs do incorporate update reviews and continuous practices, but the full extent to which they are used is unclear, and the success of their implementation is insufficient. The burden of this adjustment further highlights the need to centralize expertise and lean on automation.

230 Jai Vijayan, "SolarWinds Campaign Focuses Attention on 'Golden SAML' Attack Vector,"

DARKReading, December 22, 2020, accessed March 26, 2021, <https://www.darkreading.com/attacks-breaches/solarwinds-campaign-focuses-attention-on-golden-saml-attack-vector/d/d-id/1339794>.

231 "Federal Information Security Modernization Act," Cybersecurity and Infrastructure Security Agency, accessed March 26, 2021, <https://www.cisa.gov/federal-information-security-modernization-act>.

232 Office of the Under Secretary of Defense (Acquisition and Sustainment), *Cybersecurity Maturity Model Certification (CMMC)*, Version 1.02, March 18, 2020, Department of Defense, accessed March 26, 2021, [https://www.acq.osd.mil/cmmc/docs/CMMC\\_ModelMain\\_V1.02\\_20200318.pdf](https://www.acq.osd.mil/cmmc/docs/CMMC_ModelMain_V1.02_20200318.pdf).

233 "Frequently Asked Questions," Federal Risk and Authorization Management Program, accessed March 26, 2021, <https://www.fedramp.gov/faqs/>.

234 Defense Information Systems Agency, "Department of Defense Information Network (DoDIN) Approved Products List (APL) Process Guide," Version 2.5, July 2017, accessed March 26, 2021, [https://www.disa.mil/-/media/Files/DISA/Services/UCCO/APL-Process/APL\\_Process\\_Guide.pdf](https://www.disa.mil/-/media/Files/DISA/Services/UCCO/APL-Process/APL_Process_Guide.pdf).

**Adjust to the Digital Ecosystem:** Federal acquisition processes have long been criticized as poor fits for software because of the unique dynamism of software and its life cycle<sup>235</sup> as compared to traditional products. Moreover, as government continues to acquire and iterate more software, the magnitude of revamping policies and applying new protocols to old purchases grows increasingly expensive. The following can help government adjust to digitally oriented practices.

- **Prioritize and Secure:** Trends<sup>236</sup> in software supply chain attacks indicate a clear attacker preference: leveraging highly privileged, widely used programs. The Orion program is used by information technology (IT) departments to monitor network traffic, giving it significant access to host systems and allowing attackers to disguise the data they exfiltrated within the program's regular network traffic. Similar software compromised in state-linked incursions—CCleaner (twice),<sup>237</sup> Able Desk,<sup>238</sup> EVLog,<sup>239</sup> Vietnamese government digital signature packages,<sup>240</sup> and so on—offer deep system access and a broad (and sometimes contractually or legally obligated) userbase. The method of compromising updates and installers gives attackers access to a vast number of potential valuable targets—eighteen thousand customers in the SUNBURST campaign. Not all government-used software requires the same rigor in security, and applying controls equally to all programs is time consuming and expensive. Agencies should identify what systems and programs would be most fruitful for attackers to compromise and prioritize securing those soft spots and mitigating the consequences of their compromise first, informed in part by the threat profiles of known incursions. Such an approach also presents the opportunity for offensive components of government to provide valuable intelligence on the attack surfaces of partner agencies and help guide

235 McQuade et al., *Software Is Never Done*.

236 "Breaking Trust," Cyber Statecraft Initiative, Atlantic Council, website homepage accessed March 26, 2021, <https://www.atlanticcouncil.org/programs/scowcroft-center-for-strategy-and-security/cyber-statecraft-initiative/breaking-trust/>.

237 Lily Hay Newman, "Inside the Unnerving Supply Chain Attack That Corrupted CCleaner," *Wired*, April 17, 2018, accessed March 26, 2021, <https://www.wired.com/story/inside-the-unnerving-supply-chain-attack-that-corrupted-ccleaner/>; Lindsey O'Donnell, "Avast Network Breached As Hackers Target CCleaner Again," threatpost, October 21, 2019, <https://threatpost.com/avast-network-breached-as-hackers-target-ccleaner-again/149358/>.

238 Mathieu Tartare, "Operation StealthyTrident: corporate software under attack," welivesecurity, December 10, 2020, accessed March 26, 2021, <https://www.welivesecurity.com/2020/12/10/luckymouse-ta428-compromise-able-desktop/>.

239 "Kingslayer - A Supply Chain Attack," RSA, accessed March 26, 2021, <https://www.rsa.com/en-us/offers/kingslayer-a-supply-chain-attack>.

240 Ignacio Sanmillan and Matthieu Faou, "Operation SignSight: Supply-chain attack against a certification authority in Southeast Asia," welivesecurity, December 17, 2020, accessed March 26, 2021, <https://www.welivesecurity.com/2020/12/17/operation-signsight-supply-chain-attack-southeast-asia/>.



these efforts. The National Security Agency's (NSA's) public disclosure<sup>241</sup> of a critical vulnerability to Microsoft in January 2020 highlights the fact that US offensive elements are looking for the same exploitable flaws that defenders seek to close—in this case, a compromise in the cryptography of a Microsoft library used to verify code-signing and encrypted channels. The Vulnerabilities Equities Process (VEP), in particular, has unrealized potential to support national and industry defense with the resources of the nation's premiere offensive capabilities,<sup>242</sup> and information sharing throughout government can be improved to the same ends.

- **Define and Extend the Boundaries of Security:** The traditional concept of an acquired product as one that can be assessed, secured, and then deployed maps poorly onto software, which is frequently updated and iterated post-deployment, and the desired requirements of which are changed during development, both to the benefit of users. The security of shipped code can only be maintained through the security practices of its maintainers. The prevalence of compromised updates as an attack vector in software supply chain incidents illustrates that the security of a network extends all the way down to the security of the developer workstations maintaining its components. Thus, an emphasis on even the most basic cyber hygiene practices is needed, as several of the previously mentioned supply chain attacks can be traced back ultimately to insecure developer workstations (e.g., CCleaner) and poor cyber hygiene. Agencies must broaden their view of security in this dynamic environment and increase their rigor in verifying updates to already deployed software.
- **Audit Networks Continuously:** In line with the previously discussed Monitor Compliance Continuously section, compromise detection relies on measurements of network behavior and interaction. SCRM is ultimately an exercise in complexity management, and self-knowledge is critical to characterizing that complexity. In the case of SUNBURST, network monitoring and auditing could have detected<sup>243</sup> mismatches in login and authentication requests in Azure Active Directories or picked up on the creation of new trust entities, alerting victims to attacker behavior. It is important to note that these Golden SAML

241 National Security Agency, "Patch Critical Cryptographic Vulnerability in Microsoft Windows, Clients and Servers," Cybersecurity Advisory, January 14, 2020, accessed March 26, 2021, <https://media.defense.gov/2020/Jan/14/2002234275/-1/-1/0/CSA-WINDOWS-10-CRYPT-LIB-20190114.PDF>.

242 William Loomis and Stewart Scott, "A Role for the Vulnerabilities Equities Process in Securing Software Supply Chains," *Lawfare*, January 11, 2021, accessed March 26, 2021, <https://www.lawfareblog.com/role-vulnerabilities-equities-process-securing-software-supply-chains>.

243 Sygnia, "Detection and Hunting of Golden SAML Attack," December 2020, accessed March 26, 2021, <https://www.sygnia.co/golden-saml-advisory>.

tactics were known as early as 2017,<sup>244</sup> but also that they were not the only means of exploiting Identity and Access Management systems in Microsoft's cloud architecture. Continual assessment of network metrics can detect aberrant behavior and decrease the length of time that a compromise goes undetected. Agencies should implement such continual assessments where possible and require the same of vendors, with an eye toward identifying what trip wires are most useful to security assurance.

**Coordinate among Agencies and Network Types:** Between FISMA, FedRAMP, CMMC, SBoM, CFIUS, DoD's APL, and a dozen other procedures and policies, the minimum standards the vendors must comply with can be overwhelming. For industry, they impose barriers to entry. For government, they produce repeated work, complicate information sharing, and drain valuable staff resources. For attackers, they create confusion and inefficiency to exploit. Several coordination efforts can improve the security and efficiency of government acquisition practices, and there are several bodies well-situated to undertake the task—most notably CISA for the federal civilian agency apparatus and the Federal Acquisition Security Council (FASC) across the entire federal government.

- **Coordinate and Tier Certifications:** Many of the aforementioned processes call back to the same libraries of NIST guidelines, tailoring requirements to agency-, department-, or product-specific needs, but the advantages of common libraries are diminished when processes fail to communicate with each other. For instance, FISMA compliance only maps a vendor to a single agency, and its overlaps with DoD's CMMC requirements, which also draws from a body of NIST controls, do not carry over clearly. Between the various frameworks, there is no common approach to delineation between product, vendor, and acquiring organization, or to tiering the impact level of potential compromise or the security maturity of products or vendors. Agencies should iterate toward a centralized process that still allows custom requirements per agency-specific needs while also reducing repeated work, providing transparency to vendors, and communicating information about remarketed products to different agencies for efficiency.

244 Shaked Reiner, "Golden SAML: Newly Discovered Attack Technique Forges Authentication to Cloud Apps," CyberArk, November 21, 2017, accessed March 26, 2021, <https://www.cyberark.com/resources/threat-research-blog/golden-saml-newly-discovered-attack-technique-forges-authentication-to-cloud-apps>.

- **Centralize Information Sharing:** Successful *information and communications technology* (ICT) SCRM is ideally a whole-organization endeavor,<sup>245</sup> incorporating input from all stakeholders, including software engineers, intelligence analysts, and chief information officers (CIOs). While internally, agencies are recommended to house ICT SCRM under one body or official, they have largely failed to do so.<sup>246</sup> Among agencies, too, there is not enough communication across different network types, between offense- and defense-oriented entities, and among different auditors. Efforts to centralize communication and risk management within agencies should be replicated within the federal government as a whole, helping to alleviate chronic shortages of expertise and staff resources without sacrificing specialized knowledge of in-house networks.<sup>247</sup>
- **Build on Existing, or Potential, Successes:** It can be tempting to propose a complete overhaul of the existing, and admittedly chaotic, federal software acquisition and supply chain security regimes. To do so, though, would fail to realize programs that have begun, or are poised to begin, the tasks of improvement. A more efficient approach would draw on those successful instances and generalize their benefits throughout government. For instance, FedRAMP's "do once use many" model can help coordinate among agencies with common needs and vendors with reusable products. The General Services Administration's (GSA's) nascent Polaris program<sup>248</sup> could illustrate methods of lowering cost of entry for smaller firms, and the Vendor Risk Assessment Program (VRAP) included in it can improve information sharing within government, particularly between classified and unclassified intelligence. DoD's CMMC begins the work of tiering security practices and matching them to contract requirements while also requiring basic cyber hygiene of vendors. The FASC is well positioned to centralize ICT SCRM information sharing and acquisition coordination across the whole of government. The National Telecommunications and Information Administration (NTIA) Software Bill of Materials (SBOM) can provide a valuable deliverable metric for a vendor's capacity to track its own dependencies and for agencies to quantify their own risk exposure. CISA's EINSTEIN program could be improved to enhance network monitoring, and its National Cybersecurity Assessment and Technical Services (NCATS) offerings can assess, at

245 National Institute of Standards and Technology, "Information and Communications Technology Supply Chain Risk Management (ICT SCRM)," Department of Commerce, accessed March 26, 2021, [https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Managements/documents/nist\\_ict-scrm\\_fact-sheet.pdf](https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Managements/documents/nist_ict-scrm_fact-sheet.pdf).

246 Government and Accountability Office, *Information Technology: Federal Agencies Need to Take Urgent Action to Manage Supply Chain Risks*.

247 "Cybersecurity Skills Shortage," McAfee, accessed March 26, 2021, <https://www.mcafee.com/enterprise/en-us/about/public-policy/skills-shortage.html>.

248 General Services Administration, "Polaris GWAC Draft Request for Proposals, 47QTCB21N0002," accessed March 26, 2021, <https://sam.gov/opp/257509b8cfe14d48beb4f71033995e0b/view>.

a technical level, the security of agency networks and vendor practices. The CISA CDM initiative is intended to characterize and track agency assets and infrastructure. Whatever the specific levers of policy, legislation, and bureaucracy that must be pulled, complete overhaul is infeasible—a deliberate analysis of program successes, failures, and potential is necessary to inform sufficient and efficient hardening of the government's software supply chain vulnerabilities. Much like the development process of the software it seeks to secure, rapid and dynamic iteration and improvement of existing programs is needed to realize the potential of disparate government programs.

## Conclusion

The security of the software supply chains within the federal government is in dire need of improvement as government relies deeply on acquired software and attacks continue to mount. Fortunately, US President Joseph R. Biden, Jr.'s administration has already indicated<sup>249</sup> cybersecurity, specifically in software supply chains, will be a priority in the coming years, and the new secretary of the Department of Homeland Security is calling<sup>250</sup> for a review of the agency's EINSTEIN and CDM programs, potential points of cross-government coordination. The above lines of improvement outline the weaknesses in the state of federal acquisitions and SCRM practices and indicate broad lines of critical improvement to be pursued.

249 Eric Geller (@ericgeller), "Neuberger says the Biden admin is developing a new National Cyber Strategy that will incorporate several NSTAC recommendations, including 'promoting software and supply chain assurance' and creating a 'whole-of-nation' approach to emerging technology challenges," Twitter, February 10, 2021, 1:13 p.m., <https://twitter.com/ericgeller/status/1359566236934434817>.

250 Justin Katz, "Mayorkas calls for review of EINSTEIN, CDM," FCW, January 19, 2021, accessed March 26, 2021, <https://fcw.com/articles/2021/01/19/mayorkas-dhs-confirm-cyber.aspx?m=1>.

# Appendix C. Advancing a Data Fabric for Achieving Continuous Global Health Protection

## Overview

On January 21, 2021, US President Joseph R. Biden, Jr.'s administration released "National Security Directive 1,"<sup>251</sup> a blueprint to advance US leadership on the global stage to "strengthen the international COVID-19 response and to advance global health security and biological preparedness." The directive has several important calls to action, including the rejoining of a number of international health organizations and initiatives, as well as funding important international partnerships and accelerators that focus on therapeutics and vaccine development and distribution. The directive specifically recognizes the intertwined nature of health and wellness for the most vulnerable on the planet, the early detection and deployment of responses to mitigate pathogen and other biological threats, and the security of the United States.

One of the key directives is the establishment of the interagency National Center for Epidemic Forecasting and Outbreak Analytics (NCEFOA) that will help implement "global early warning and trigger systems for scaling action to prevent, detect, respond to, and recover from emerging biological threats." The NCEFOA's forecasting and early warning system echoes the Atlantic Council's call to action for the establishment of a global system for detection, warning, and mitigation. Vaccine and therapeutic development and distribution are identified as key parts of the mitigation response.

Such a bold plan is inherently a data-centric plan, one which will require a responsive network architecture to maintain the key tenets of cybersecurity, interoperability, and the ability to deploy algorithmic intelligence and artificial intelligence (AI) at the edge. This approach proposes an inherently cybersecure network architecture, initially funded by the National Science Foundation (NSF), to solve this problem.

251 Federation of American Scientists, "National Security Directive on United States Global Leadership to Strengthen the International COVID-19 Response and to Advance Global Health Security and Biological Preparedness," National Security Directive - 1, January 21, 2021, accessed March 26, 2021, <https://fas.org/irp/offdocs/biden-nsd/nsd-1.pdf>.

Named Data Networking (NDN)<sup>252</sup> is a future Internet architecture whose development was inspired by the recognition of unsolved problems and inherent security risks in the current Internet architecture. One of the fundamental uses of the Internet is to distribute information. The current schema of the Internet is to perform data sharing based on an Internet Protocol (IP) address, or where the data resides. This is *not content secure*, and a number of Band-Aid solutions have been deployed to fix this. These have not proven very effective, as the innumerable hacks of the US healthcare system have demonstrated. These attacks have gone so far as to bring healthcare systems to their knees,<sup>253</sup> infiltrate critical medical supply chains [COVID-19 vaccine cold-chain distribution<sup>254</sup> and personal protective equipment (PPE) procurement<sup>255</sup>], and harvest valuable research and development (R&D) and intellectual property around vaccine development.<sup>256</sup> None of this is compatible with the United States' elevated cybersecurity needs.

NDN, as an Internet architecture, can only be made fully operational with edge devices if a federated identity management system (FIMS) is enabled; this will ensure that data producers at the edge (i.e., humans, healthcare systems, data servers, Internet of Things devices) can be authenticated, and the data they produce wrapped in an individual security wrapper. The data produced is also immutable, version tracked, and cryptographically signed. If such a system were to be hacked, or subject to a ransomware attack, it would not matter, because each piece of content within that container would be protected with these additional layers of security. Further, that data could be logically distributed and stored, and combined only when necessary, e.g., for data aggregation, AI applications, and sense-making. Finally, by securing and addressing data by content, the producers at the edge can become data owners. That means, citizens or municipalities whose healthcare data are interacting with the system at the edge can own encrypted versions of their personal data that are similarly difficult to hack, and then transact with it. In the process of securing the data with this alternate

252 "Named Data Networking: Motivation & Details," Named Data Networking, accessed March 26, 2021, <https://named-data.net/project/archoverview/>; "NDN Community Meeting, September 10-11, 2020," NIST, accessed March 26, 2021, <https://www.nist.gov/news-events/events/2020/09/ndn-community-meeting>; Cameron Ogle et al., "Named Data Networking for Genomics Data Management and Integrated Workflows," *Frontiers in Big Data*, February 15, accessed March 26, 2021, <https://www.frontiersin.org/articles/10.3389/fdata.2021.582468/full>.

253 Jessica Davis, "UPDATE: The 10 Biggest Healthcare Data Breaches of 2020, So Far," *HealthITSecurity*, July 8, 2020, accessed March 26, 2021, <https://healthitsecurity.com/news/the-10-biggest-healthcare-data-breaches-of-2020-so-far>.

254 Cybersecurity and Infrastructure Security Agency, "IBM Releases Report on Cyber Actors Targeting the COVID-19 Vaccine Supply Chain," original release date: December 03, 2020, accessed March 26, 2021, <https://us-cert.cisa.gov/ncas/current-activity/2020/12/03/ibm-releases-report-cyber-actors-targeting-covid-19-vaccine-supply>.

255 Rich Haridy, "COVID-19 vaccine distribution networks targeted by hackers," *New Atlas*, December 3, 2020, accessed March 26, 2021, <https://newatlas.com/computers/hackers-target-covid-19-vaccine-distribution-networks/>.

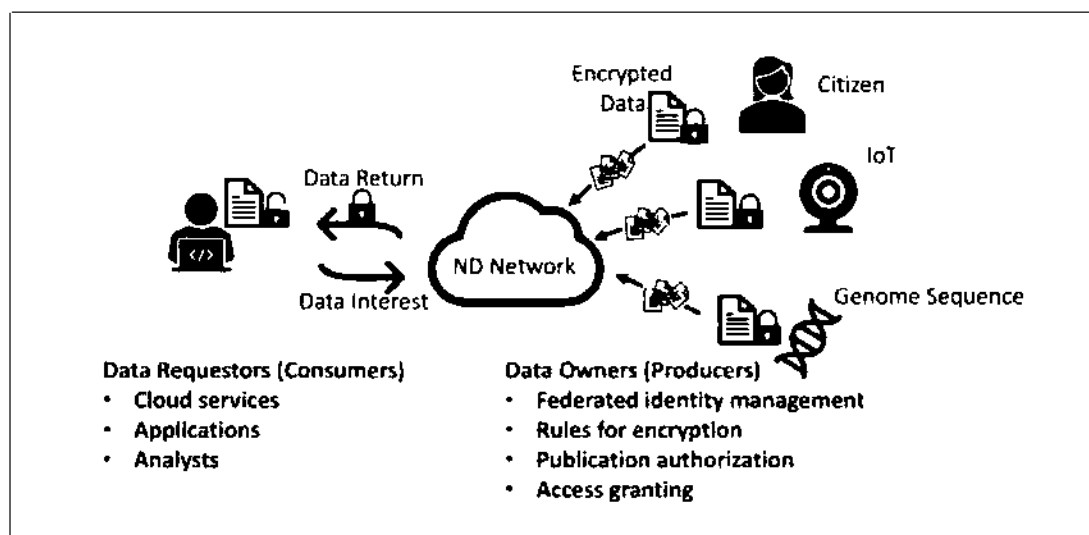
256 James Purtill, "Cozy Bears and Hidden Cobras: The hackers targeting COVID-19 vaccine researchers," *ABC Science*, December 14, 2020, accessed March 26, 2021, <https://www.abc.net.au/news/science/2020-12-15/covid-19-coronavirus-the-hackers-targeting-vaccine-researchers/12974504>.

Internet architecture, a mechanism for establishing data trusts and only sharing necessary data is enabled. This model of data ownership further enables a type of fiduciary trust in which even public-private partnerships (PPPs) will not result in private interests capturing data for commercial or shareholder interests.

Thus, a content-based Internet data fabric with edge device security and authentication provides these value propositions:

- Establishment of a “total trust network” comprising independently owned and authorized private vaults that share a common security and information framework;
- Trusted user, device, and application identity, e.g., human, computer, IoT, sensors;
- Data owner/producer-controlled data sharing and exposure based primarily on the entity and/or transaction—the who, what, when, and how;
- Fully protected data exchange, verification, and immutability between authorized entities available anywhere and anytime, without the threat of data leaks, ransomware, or hacking;
- Easy integration into existing networks;
- Deployment on any private or public cloud architecture; and
- Support for all existing supplementary authentication methodologies (e.g., multifactor).

**Figure C.1: Schematic for Secure Network with Data Producers and Consumers**

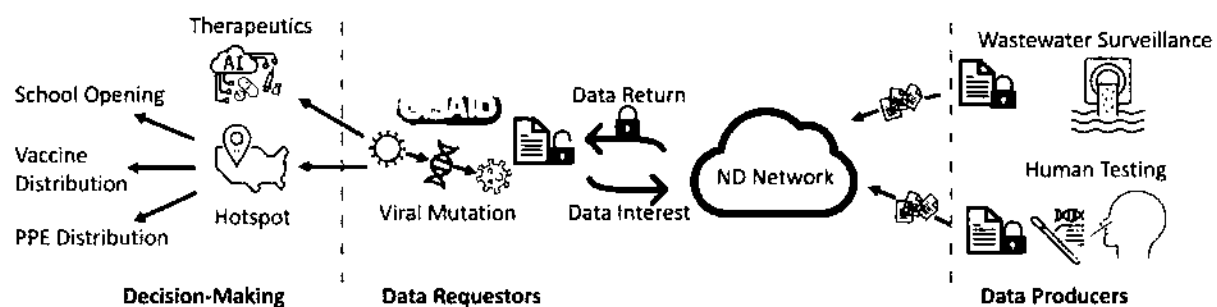


This work proposes two testbed models for this future Internet architecture to secure the United States’ critical healthcare data and infrastructure.

### Model 1: Testbed for the National Center for Epidemic Forecasting and Outbreak Analytics (NCEFOA) to prevent, detect, respond to, and recover from emerging biological threats.

The first model is a wastewater surveillance and pathogen sequencing/mutation network, in which municipal wastewater surveillance can be combined with individual viral testing and sequencing. Such data might be requested by federal, state, and local health agencies to identify hot spots early and track viral mutations by locale. It would also enable the detection of novel pathogens by sequence. This information may then be used to direct the development of AI-based therapeutics and critical policy and economic decision making, such as driving alert systems, directing school and business openings, and identifying vulnerable zip codes for rapid vaccine/therapeutics distribution, as well as healthcare resource distribution such as PPE, medical personnel, beds and ventilators.

Figure C.2: Wastewater Surveillance and Viral Mutation Integration Network

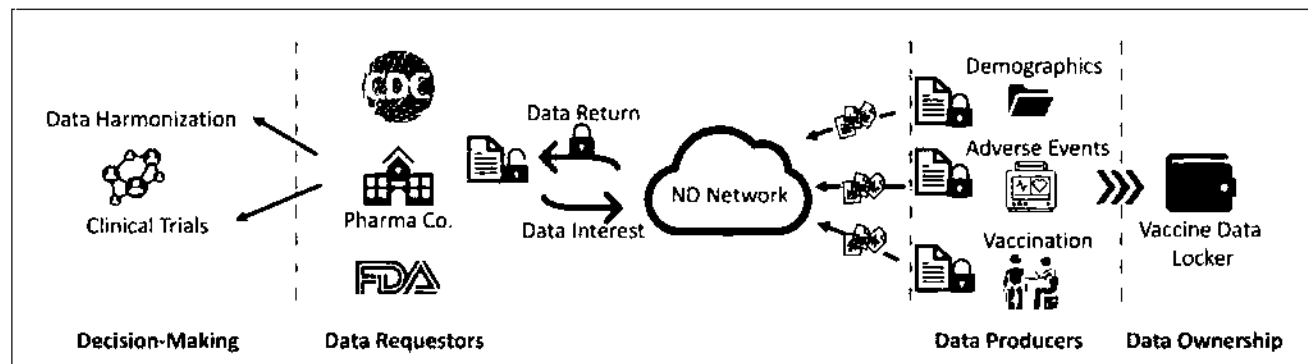


### Model 2: Testbed for a response to coordinate vaccine and therapeutic development and distribution.

The second model is a vaccine distribution application based on the enhanced cybersecurity provided by the NDN. This application would enable both the tracking of vaccine (lot, dose, timing) and recipient demographics (source encryption). It would further enable data harmonization and a system for reporting adverse viral events to health officials, the Centers for Disease Control and Prevention (CDC), the Food and Drug Administration (FDA), and to pharma companies, so they can continue to perform Phases III and IV clinical trials in the pursuit of FDA clearance and human safety. The vaccine tracking system would also enable tracking of surplus vaccine for eventual donation to global vaccine pools. Early deployment would be compatible with the Federal Emergency Management Agency (FEMA)-based vaccination centers announced by the Biden administration. Alternatively, the application could be deployed on the vaccine provider side to assist with the distribution of vaccines in underserved areas within the United States (e.g., rural areas, Navajo Nation).



Figure C.3: Vaccine Distribution Network Application with Vaccine Data Lockers



A key element is an advanced polymorphic trust network architecture that is decentralized, reliable, resilient, and cybersecure to enable the administration to reach key goals within “National Security Directive-1.” The trust network architecture is virtually impervious to hacking and ransomware attacks because the data are immutable and signed. In addition, there are two model testbeds that answer needs within the directive—one for early detection and warning, by combining wastewater surveillance, pathogen testing, and mutation analysis; and the second for vaccine distribution, adverse events reporting, and data ownership, that would also enable pharma to conduct ongoing, secured, digital clinical trials. The system also provides for implementing a public data trust, within a decentralized system, in which much of the fiduciary responsibility for the data lies in the naming and immediate securing of sensitive, immutable data as it is generated, and identity management and authentication of key stakeholders. This permits data sharing only between authenticated producers and receivers, and removes the data profit or surveillance motive in gathering data for critical intelligence. Often these types of data gathering do not reconcile well with the cornerstones of democracy, such as public ownership and participation. The network architecture is compatible with the seemingly opposing directives of intelligent surveillance and civil liberties.

This framework delivers a virtually impenetrable mechanism with a higher degree of trust that is essential to securing our cyberhealth and R&D, and digitally transacting with sensitive biometric data. It will enable the United States to move forward with data-centric policies that both enable edge data intelligence and integration of new and existing networks involved in sensing capabilities, while protecting Americans’ civil liberties. Furthermore, it provides a new, secure network architecture that can integrate the vast number of sensors and bidirectional IoT devices coming online. In addition to securing the United States’ cyberhealth infrastructure, the network architecture plus federated identity management and authentication would be valuable for securing infrastructure, communications, sensor data, voting data, and enabling things like digital identities, commerce, and banking.

# Appendix D. Additional Readings on the History and Future of Global Space Governance

---

By 2050, numerous studies indicate that the commercial space industry will reach a valuation of more than \$3 trillion. In response, there has been much interest among policy makers in the potential geopolitical, economic, and social ramifications that will result from this expansion. In their attempts to quickly tap into this market, however, there has been one area that has yet to receive much scrutiny: the space governance regime itself. As more private industries expand into this domain, they are likely to run into an outdated governance regime that has seen little modification since the Cold War. Drafted and codified in an era when space was dominated by two major nation-states, these regulations have yet to be framed to reflect a new era of space commercialization and management. Unaddressed, inflexibilities in the current regime could hinder the successful development of outer space, creating a range of problems for both the private and public sectors. While broad solutions have yet to be found, any well-informed debate on the future of space must include discussions on the challenges of governing space, issues that have vexed policy makers since the 1950s. For the GeoTech Decade, leaders from all sectors, nations, and industries must be aware of the hazards and potential solutions ahead. Listing from chronological order from 2015 to 2021, plus one entry from 2011, the following readings represent scholarly research on this evolving topic area.

## **1. Toward a Theory of Space Power: Selected Essays**

Editors: Charles D. Lutes, Peter L. Hays, Vincent A. Manzo, Lisa M. Yambrick, and M. Elaine Bunn

Publication date: 2011

Publisher: National Defense University Press, Washington, D.C.

Excerpts from the publication:

Chapter 3: International Relations Theory and Space Power (Robert L. Pflatzgraff Jr.)

“Because the stakes are immense, how we theorize about space, drawing on existing and yet-to-be-developed IR and other social science theories, will have major implications for strategies and policies. Because no single IR theory capable of describing, explaining, or prescribing political behavior on Earth exists, we cannot expect to find otherwise in space. Therefore, it is important to recognize the inherent limitations in extrapolating from Earthly IR theory to space, while also drawing wherever possible on such theory as we probe farther into space.”

Chapter 11: Merchant and Guardian Challenges in the Exercise of Space Power (Scott Pace)

“[T]he Outer Space Treaty, by barring claims of sovereignty, is usually thought to bar private property claims. Many legal scholars in the International Institute of Space Law and other organizations support that view. Other scholars, however, make a distinction between sovereignty and property and point to civil law that recognizes property rights independent of sovereignty. It has also been argued that while Article II of the treaty prohibits territorial sovereignty, it does not prohibit private appropriation. The provision of the Outer Space Treaty requiring state parties to be responsible for the activities of persons under their jurisdiction or control leaves the door open to agreements or processes that allow them to recognize and confer property rights, even under common law.

“Current international space treaties are built on the assumption that all matters can and should trace back to states. This is in contrast to admiralty law and the growing field of commercial arbitration in which the interests and responsibilities of owners, not necessarily the state, were the legal foundation. It can be argued that the Outer Space Treaty was not the final word on real property rights in space even within the international space law community, as drafters of the 1979 Moon Treaty felt it necessary to be more explicit on this point.

“Legal issues will become increasingly more important as the ‘Vision for Space Exploration’ proceeds and humans attempt to expand farther and more permanently into space. In exercising spacepower, the United States should seek to ensure that its citizens have at least as many rights and protections in space, including the right to own property, as they do on Earth. Whether such rights would be as complete as those in the United States would be the subject of negotiation and debate. Simply put, however, the Moon and other celestial bodies should not be a place of fewer liberties than those enjoyed on Earth.”

Link: <https://ndupress.ndu.edu/Portals/68/Documents/Books/spacepower.pdf>

## **2. 'How Simple Terms Mislead Us: The Pitfalls of Thinking About Outer Space as a Commons'**

Authors: Henry R. Hertzfeld, Brian Weeden, and Christopher D. Johnson

Publication date: 2015

Publisher: Secure World Foundation

Excerpt from the publication:

"Thinking about space as a global commons may be a laudatory ideal, and one that perhaps can be regarded as a very long-term goal for society. But it is hardly a practical solution or goal for the problems we face today, witnessed by at least a thousand years of precedent in law and practice coupled with radically different technologies, exponential world population growth from 500 million people (at most) in Roman times and the Middle Ages to over 7 billion people today, and other radical political and social changes.

"But all of the ways we try to phrase 'benefits to all mankind,' 'province of all mankind,' etc. have their limits. Treaty guarantees such as no sovereignty are not the same as limiting ownership, property rights, and establishing the concept of national liability for activities and human behavior in space.

"Attempts to develop some sort of overall 'governance' of space based on a res communis principle will not succeed in today's political environment. (Or, quite likely in any form where nations have the ability to interpret treaty language differently and where different forms of government exist.)"

Link: <https://swfound.org/media/205390/how-simple-terms-mislead-us-hertzfeld-johnson-weeden-iac-2015.pdf>

## **3. National Security Space Defense and Protection**

Publication Date: 2016

Publisher: The National Academies Press

Excerpt from the publication:

"The significant difference, of course, between the creation of global maritime policy and practice and that of the space domain is time. The technologies, customary behaviors, conventions and, eventually, treaties governing military and commercial naval activity evolved over centuries along with the enabling operational concepts, naval strategies, nation-states and attendant diplomacy. The system was thus able to gradually incorporate advances, slowly accommodate stresses, and, to some degree, resolve conflicts in a deliberate manner over time.

"A key aspect of space is that the speed of advances in access and space-borne capabilities has significantly outpaced the creation of guiding national-let alone international strategies and policies. The technological advances in space

systems and increased reliance on them have created a space-enabled ‘critical infrastructure’ that has not been matched by coherent supporting protection and loss-mitigation strategies, clearly articulated and accepted policies, and robust defensive capabilities. These gaps have created newfound concern domestically, confusion on the part of allies, and opportunities for misalignment and misperceptions on the part of potential adversaries. The need to rapidly, precisely, and effectively address all of these factors has created an environment of urgency to find mitigation strategies, fill policy gaps, and fund new capabilities. Done poorly, rapid efforts and expansive rhetoric can exacerbate existing tensions, pursue capabilities that add only marginally to system security, and increase the probability of misunderstanding or miscalculation on the part of potential adversaries. Well coordinated and properly executed, these efforts can meet real needs, add essential system security, and promote stability. These efforts must succeed. National security and global stability in space and on Earth demand it.”

Link: <https://doi.org/10.17226/23594>

#### **4. ‘Space Development, Laws, and Values’**

Author: Scott Pace, executive secretary, National Space Council

Date: December 13, 2017

Details: Speech to the IISL Galloway Space Law Symposium, Cosmos Club, Washington, DC

Excerpt from the speech:

“[I]n today’s world, technology and entrepreneurship threaten to outpace the legal and domestic regulatory mechanisms intended to enable and manage space activities. When technological generations occur every 18 months or so, it would appear to outside observers that the pace of international space discussions at the United Nations is, by comparison, glacial. As many of you know, the development of voluntary ‘best practices’ for the long-term sustainability (LTS) of outer space activities at the UN Committee on the Peaceful Uses of Outer Space is expected to be finalized next year after years of cooperative, but sometimes contentious, efforts. In the intervening time since LTS discussions began, we have seen many new developments, from new space start-ups, reusable rockets, and proposals for mega-constellations, alongside more traditional governmental space activities.

“U.S. leadership requires active engagement in interpreting and implementing existing space agreements and other international law, while pursuing non-binding ‘best practices’ and confidence-building measures with our allies, security partners, and potential adversaries to meet today’s space challenges. It necessitates enacting transparent, effective, and minimally burdensome domestic legislation and regulatory mechanisms to enable U.S. companies to benefit from technology development and new commercial opportunities.”

Link: <https://spacepolicyonline.com/wp-content/uploads/2017/12/Scott-Pace-to-Galloway-FINAL.pdf>

## 5. Handbook for New Actors in Space

Editor: Christopher D. Johnson

Publication date: 2017

Publisher: Secure World Foundation

Excerpt from passage:

“Space is changing. The barriers to access to space are decreasing. Shrinking costs, less infrastructure, and lower technological hurdles all make space activities available to more people. Meanwhile, smaller programs with fewer necessary personnel enable more states and entities to participate in space projects. Nevertheless, regardless of a space project's size, the existing international legal and regulatory framework underpins and permits space activities. This regime is decades old and was created in a different geopolitical context. Some feel it is ill-suited for the next half-century of space activities—either too restrictive, or not sufficiently clear in its requirements.”

Link: <https://commons.erau.edu/cgi/viewcontent.cgi?article=1006&context=db-cso-351-spring2019>

## 6. ‘Space, the Final Economic Frontier’

Author: Matthew Weinzierl

Publication date: 2018

Publisher: *Journal of Economic Perspectives*, Volume 32, Number 2, Pages 173-192

Excerpt from the publication:

“The vulnerabilities of centralized control will be familiar to any economist: weak incentives for the efficient allocation of resources, poor aggregation of dispersed information, and resistance to innovation due to reduced competition. In addition to these concerns, NASA's funding and priorities were subject to frequent, at times dramatic, revision by policymakers, making it hard for the space sector to achieve even the objectives set at the center (Handberg 1995; Logsdon 2011).

“Anticipating these vulnerabilities, reform advocates had made previous pushes for at least partial decentralization and a greater role for the private sector in space. Near the dawn of the Shuttle era, President Ronald Reagan signed the Commercial Space Launch Act of 1984, saying: ‘One of the important objectives of my administration has been, and will continue to be, the encouragement of the private sector in commercial space endeavors.’ That same year saw the creation of the Office of Commercial Programs at NASA and the Office of

Commercial Space Transportation in the Department of Transportation (NASA 2014). However, these early seeds would have to wait until the end of the Shuttle program to bear fruit.”

Link: [https://www.hbs.edu/ris/Publication%20Files/jep.32.2.173\\_Space,%20the%20Final%20Economic%20Frontier\\_413bf24d-42e6-4cea-8cc5-a0d2f6fc6a70.pdf](https://www.hbs.edu/ris/Publication%20Files/jep.32.2.173_Space,%20the%20Final%20Economic%20Frontier_413bf24d-42e6-4cea-8cc5-a0d2f6fc6a70.pdf)

## **7. ‘Space Technology and the Implementation of the 2030 Agenda’**

Author: Simonetta DiPippo

Publication date: 2019

Publisher: *UN Chronicle*, Volume 55, Issue 4, Pages 61-63

Excerpt from the publication:

“There are already many tangible changes and challenges to the traditional ways of conducting space activities, with many new actors entering the field and new technologies affecting our efforts. When the space age began with the launch of Sputnik 1 in 1957, only two countries were active in the space environment. Today, we have over 70 national and regional space agencies working to extend our knowledge of space and apply space science and technology to improve the lives of people worldwide. Thousands of other actors are also joining the space community, with a well-established private space sector.

“With the rapid expansion of stakeholders accessing space, the estimated value of the space sector reached an all-time high of \$383.5 billion in 2017, with commercial space activities accounting for over 75 per cent of that value. Such statistics demonstrate the extent to which private entities have become major players in the field. Projections for the future value of the sector show it rising at an exponential pace, reaching \$1.1 trillion to \$2.7 trillion over the next 30 years.”

Link: <https://www.un.org/en/chronicle/article/space-technology-and-implementation-2030-agenda>

## **8. 'Catalyzing Space Debris Removal, Salvage, and Use'**

Authors: Peter Garretson, Alfred B. Anzaldúa, and Hoyt Davidson

Publication date: 2019

Publisher: *The Space Review*

Excerpt from the publication:

"[S]alvage and debris cleanup is very difficult under the current international legal space regime and orbital conditions, all of which disincentivize action. First, per Article VIII of the Outer Space Treaty (OST), a State Party on whose registry an object is launched into outer space retains jurisdiction and control of the items launched. Moreover, Articles VI and VII of the OST and Article IV of the Liability Convention make multiple launching states involved in a space debris intervention jointly and severally liable for any harm or damage to the persons or property of other States Parties.

"Further complicating liability assessment, a lot of orbital debris is unclaimed and neither the spacecraft owner nor operator nor the launching state can be determined. According to Brian Weeden of the Secure World Foundation, 'Of the 500,000 estimated human-generated objects in orbit bigger than one centimeter, we only know which country put it there for about 16,000 objects. And less than half of those 16,000 were registered with the UN.' Moreover, deorbiting debris will often require moving the junk through lower orbits. Further aggravating the issue, moving debris to salvage yards for later use will sometimes require moving the debris through higher orbits. In each case, there will likely be an increased risk of collision or other accidents.

"While it may be unclear if anyone is liable for unclaimed debris, it can be argued that the moment a State Party to the OST, via its national entity, touches the debris, the State Party assumes liability for whatever happens according to Article VI of the OST, which mandates that State Parties bear 'international responsibility' for national activities in outer space and also requires 'authorization and continuing supervision' of the involved national actors."

Link: <https://www.thespacereview.com/article/3847/1>

## **9. War in Space: Strategy, Spacepower, Geopolitics**

Author: Bleddyn E. Bowen

Publication date: 2020

Publisher: Edinburgh Press



Excerpt from the publication:

“Today, over 2,000 active satellites are deployed in Earth orbit by over seventy states and commercial entities. The global space economy in 2018 was worth around US\$360 billion. The uses of satellites and the potential consequences of their denial in a time of war are generating strategic effects that strategists and scholars must account for. The infrastructural and support services derived from orbital satellite constellations remains an under-theorised and under-conceptualised techno-geographic phenomenon in IR and strategic studies. These satellites provide a range of functions for military, economic, civilian, intelligence and scientific needs.

“The proliferation of those technologies outside the United States is eroding one of the main advantages Western militaries have enjoyed since the end of the Cold War, levelling somewhat the conventional military and economic balances of the ‘great powers’ with significant implications for global power relations in the twenty-first century. Earth’s major powers are exploiting their own space infrastructure and pursuing space weapons technology which have undermined an oft-assumed American dominance of outer space, but it has not necessarily ended American power preponderance on Earth”

Link: <https://marketplace.officialstatistics.org/privacy-preserving-techniques-handbook>

## **10. ‘Executive Order 13914 of April 6, 2020: Encouraging International Support for the Recovery and Use of Space Resources’**

Author: United States Government

Publication date: April 6, 2020

Publisher: Executive Office of the President, United States Government

Excerpt from the Executive Order:

“Successful long-term exploration and scientific discovery of the Moon, Mars, and other celestial bodies will require partnership with commercial entities to recover and use resources, including water and certain minerals, in outer space.

“Uncertainty regarding the right to recover and use space resources, including the extension of the right to commercial recovery and use of lunar resources, however, has discouraged some commercial entities from participating in this enterprise. Questions as to whether the 1979 Agreement Governing the Activities of States on the Moon and Other Celestial Bodies (the ‘Moon Agreement’) establishes the legal framework for nation states concerning the recovery and use of space resources have deepened this uncertainty, particularly because the United States has neither signed nor ratified the Moon Agreement. In fact, only 18 countries have ratified the Moon Agreement, including just 17 of the 95 Member States of the United Nations Committee on the Peaceful Uses of Outer Space.

Moreover, differences between the Moon Agreement and the 1967 Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies—which the United States and 108 other countries have joined—also contribute to uncertainty regarding the right to recover and use space resources.”

Link: <https://www.federalregister.gov/documents/2020/04/10/2020-07800/encouraging-international-support-for-the-recovery-and-use-of-space-resources>

## 11. ‘Space Governance in the New Space Era’

Authors: Daniel L. Oltrogge and Ian A. Christensen

Publication date: 2020

Publisher: *Journal of Space Safety Engineering*, Volume 7, Issue 3, Pages 432-438

Excerpt from the publication:

“Applied to space activities, adaptive governance is the idea that ‘you can’t effectively regulate what you don’t know’ (e.g., technological approaches, business models); yet for new applications, regulations are needed to provide legal certainty and common rules and to satisfy international obligations. Achieving this balance requires a system of regular updates to regulatory provisions and frameworks, rather than attempts to address new applications in totality. It also requires exchanges of information between technical, economic, business, policy and regulatory communities. It is a philosophy of governance, rather than specific structure or approach. For example, an international working group developing a set of legal building blocks to enable commercial utilization of space resources has found that it is ‘neither necessary nor feasible to attempt to comprehensively address space resource activities in the building blocks: space resource activities should be incrementally addressed at the appropriate time on the basis of contemporary technology and practices’”

Link: <https://www.sciencedirect.com/science/article/pii/S2468896720300550?via%3Dihub>

## 12. ‘The US National Space Policy (2020)’

Authors: United States Government

Publication date: 2020

Publisher: Executive Office of the President, United States Government

Excerpt from the publication:

“It is the policy of the United States to ensure that space operations are consistent with the following principles.

(1) It is the shared interest of all nations to act responsibly in space to ensure the safety, stability, security, and long-term sustainability of space activities. Responsible space actors operate with openness, transparency, and predictability to maintain the benefits of space for all humanity.

(2) A robust, innovative, and competitive commercial space sector is the source of continued progress and sustained United States leadership in space. The United States remains committed to encouraging and facilitating the continued growth of a domestic commercial space sector that is globally competitive, supports national interests, and advances United States leadership in the generation of new markets and innovation-driven entrepreneurship.

(3) In this resurgent era of space exploration, the United States will expand its leadership alongside nations that share its democratic values, respect for human rights, and economic freedom. Those values will extend with us to all space destinations as the United States once again steps beyond Earth, starting with the Moon and continuing to Mars.

(4) As established in international law, outer space, including the Moon and other celestial bodies, is not subject to national appropriation by claim of sovereignty, by means of use or occupation, or by any other means. The United States will pursue the extraction and utilization of space resources in compliance with applicable law, recognizing those resources as critical for sustainable exploration, scientific discovery, and commercial operations.

(5) All nations have the right to explore and to use space for peaceful purposes and for the benefit of all humanity, in accordance with applicable law. Consistent with that principle, the United States will continue to use space for national security activities, including for the exercise of the inherent right of self-defense. Unfettered access and freedom to operate in space is a vital national interest.

(6) The United States considers the space systems of all nations to have the right to pass through and conduct operations in space without interference. Purposeful interference with space systems, including supporting infrastructure, will be considered an infringement of a nation's rights. Consistent with the defense of those rights, the United States will seek to deter, counter, and defeat threats in the space domain that are hostile to the national interests of the United States and its allies. Any purposeful interference with or an attack upon the space systems of the United States or its allies that directly affects national rights will be met with a deliberate response at a time, place, manner, and domain of our choosing."

Link: <https://www.federalregister.gov/documents/2020/12/16/2020-27892/the-national-space-policy>

### **13. Responsible Space Behavior for the New Space Era: Preserving the Province of Humanity**

Authors: Bruce McClintock, Katie Feistel, Douglas C. Ligor, and Kathryn O'Connor

Publication date: 2021

Publisher: RAND Corporation

Excerpt from the publication:

“In the early days of space exploration, few actors had the resources and motivation to place satellites on orbit. Therefore, there was less concern over space traffic, and the focus was primarily on tracking satellites with basic position information to send and receive information or commands. As space has become more congested, the importance of safety from collisions has increased in importance. Safety in space hinges on the ability to carry out a satellite's mission without unintentional interference. The growing number of space actors, space objects, and space debris in the New Space Era creates challenges for operating safely in space. To provide a sense of magnitude, some estimate that 96 percent of space objects are untracked and the number of satellites on orbit could increase by four to ten times in the next decade. Maintaining a safe environment in space requires a chain of interconnected activities that includes detection, tracking, communication and coordination between users, and, if necessary, commands to maneuver satellites to prevent potential collisions. There is also the need for more debris management to mitigate the ever-increasing buildup of inactive objects in space. Nearly every step in this chain has shortcomings, so there is a compelling need to improve overall safety activities.”

Link: <https://www.rand.org/pubs/perspectives/PEA887-2.html>

#### **14. The Outer Space Treaty: Overcoming Space Security Governance Challenges**

Author: Rajeswari Pillai Rajagopalan

Publication date: 2021

Publisher: Council on Foreign Relations

Excerpt from the publication:

“These trends are proving to be a growing challenge for existing global governance mechanisms. Outer space activities are governed by a number of treaties and agreements, the foundation of which is the 1967 Outer Space Treaty (OST)—or, more formally, the Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies. But these agreements were developed in the 1960s and 1970s, and they are showing their age. Constructed under different geopolitical and technological circumstances, they are not well-suited for addressing contemporary challenges.

“Legally binding measures, including revising the OST, should be pursued in earnest, but the political impediments to developing new measures or amending existing measures are challenging to overcome. Given that the difficulties arise mostly from political disagreements, nonlegal, political instruments such as transparency and confidence-building measures (TCBMs) should also be pursued. While legal measures such as reforming the OST still need to be considered the end goal, this working paper recommends a step-by-step approach to addressing the political difficulties of developing effective rules of the road.

“Two opposing perspectives prevail on global governance in outer space—one that believes that legal measures are necessary to resolve the problems facing the current space regime and another that argues that, given the contemporary political climate, traditional TCBMs are the more practical goal.”

Link: <https://www.cfr.org/report/outer-space-treaty>

# Appendix E. Informational GeoTech Center Synopses

## 1. 5G's Geopolitics Solvable by Improving Routing Protocols against Modern Threats<sup>257</sup>

Author: David Bray, PhD

April 9, 2020

The article is accessible at:

<https://www.atlanticcouncil.org/blogs/geotech-cues/5gs-geopolitics-solvable-by-improving-routing-protocols-vs-modern-threats>

This article addresses the fear, uncertainty, and doubt that have been cast on the 5th Generation of International Mobile Telecommunications standards (5G), which has become a geopolitical point of contention between China and the United States. 5G standards themselves still have to be finalized internationally, making it even more difficult to discern market reality versus market positioning versus market hype.

As such, having performed a deeper dive into the issues surrounding 5G over the last few months, the GeoTech Center proposes to global policy makers that the geopolitical tensions associated with 5G, as well as other geopolitical cybersecurity-related concerns, can be solved by improving routing protocols against modern threats. Such an endeavor would require a commitment from multiple parties to advance the state-of-the-art in content- and trust-based routing protocols in terms of research and development, with an eye to future benefits in three to five years.

The purpose of this article is to motivate global policy makers and industry leaders to develop and demonstrate a governance protocol by which an individual communications network device can evolve one or more trustworthy communication pathways in a heterogeneous communications environment amid potentially deceptive and disruptive nodes.

Key conclusions include the following:

<sup>257</sup> David Bray, "5G's geopolitics solvable by improving routing protocols against modern threats," Atlantic Council, April 9, 2020, accessed March 26, 2021, <https://www.atlanticcouncil.org/blogs/geotech-cues/5gs-geopolitics-solvable-by-improving-routing-protocols-vs-modern-threats/>.

- If consumers or markets are concerned that 5G technologies are being used surreptitiously for intelligence purposes without their consent, that will erode trust in open societies and free markets.
- Internet-based routing includes the Border Gateway Protocol (BGP). Unfortunately, BGP lacks cryptographic identification that can prove Autonomous Systems (ASes) providing routing information are who they claim or that the information they provide on behalf of other ASes can be trusted. To fix this, Secure BGP and related approaches attempt to overcome the vulnerabilities present in BGP, yet so far Secure BGP and similar efforts to address these vulnerabilities have proven economically difficult to deploy at scale. Even then, like BGP, Secure BGP itself has limits on the growth of the routing table.
- 256 GB of NAND flash memory simply has not been available for most of the history of the Internet and mobile communications; now it is available cheaply and will continue getting cheaper as data centers are driving this decrease in cost. NAND stores data in arrays of memory cells that are made using floating-gate transistors.
- At the same time, 5G should reduce latency and increase bandwidth. As a result, sending out exploratory packages is now possible for densely connected workers in ways that were not possible with 2G or 3G. Also, onboard computing is able to do more than what was possible in the past; a palm-size device now does twenty teraflops using x86 architectures at low energy/via solar power.
- Regardless of 5G, 4G, or any other mobile telecommunications standards, the era in which on-system memory limits prevented storing the necessary information about potential nodes from which to evolve trust is over.

## 2. Space Salon: Making Space Available to Everyone<sup>258</sup>

Panelists: Joseph Bonivel, Jr., nonresident senior fellow at the Atlantic Council's GeoTech Center; Paul Jurasin, director of New Programs/Digital Transformation Hub at Cal Poly State University; Jody Medich, principal design researcher, Microsoft Office of the CTO; Michael Nicolls, principal engineer at SpaceX and founding CTO of LeoLabs, Inc.; and Simon Reid, chief operating officer, D-Orbit UK.

July 8, 2020

The recording is accessible at the following link:

258 Atlantic Council, "Space salon: Making space available for everyone," July 8, 2020, accessed March 26, 2021, <https://www.atlanticcouncil.org/event/space-salon-making-space-available-for-everyone/>.

<https://www.atlanticcouncil.org/event/space-salon-making-space-available-for-everyone/>

In this event, panelists discuss how space operations are transitioning from an industry heavily driven by government funding and strategy to a commercially focused and self-sufficient market. The private sector now regularly invests in rockets, satellite hardware, and experiments in space to advance its business interests, driving a shift in how the space industry operates and thrives. As the National Aeronautics and Space Administration (NASA) and other space agencies gradually transition responsibility for orbital safety activities to the commercial world, private companies will increasingly assume the risks of space travel and operations in space.

The event concluded that:

- The current period marks the beginning of space commercialization. Innovation as well as novel applications of existing technology, such as using virtual reality (VR) to accelerate training for space operators, will continue to lower barriers to entry. Nevertheless, both commercial and government actors can take actionable steps to make space available for everyone.
- There remain significant barriers to entry in the commercial space sector. Of course, the physical requirements to launch a satellite into low-Earth orbit are substantial, intensified by multiplying debris in space. Government regulatory hurdles further dissuade firms from potentially entering the commercial space sector. Future efforts must be aimed at reforming regulation to encourage competition and innovation.
- A lack of data standardization may hinder innovation in space. Private companies gather massive amounts of satellite data which largely remains siloed on company servers. Industry must develop its own open-source data standards to foster collaboration. Governments should step in later, recognizing that industry moves faster. Once standards are developed, firms should move toward building networks of satellites with integrated sensors and automated collision avoidance systems.
- Governments must facilitate innovation, promote transparency, and ensure equitable access to space. Updating regulatory frameworks to encourage responsible private sector coordination represents a promising first step. Governments should also begin sharing more data to promote transparency. Lastly, governments need to adopt policies on space commercialization that benefit everyone: a rural farmer should have just as much access to data collected in space as a multinational corporation.



### 3. Building a Collaborative Ecosystem for AI in Healthcare in Low- and Middle-Income Economies<sup>259</sup>

Authors: Abhinav Verma, Krisstina Rao, Vivek Eluri, and Yukti Sharma

August 27, 2020

The article is accessible at:

<https://www.atlanticcouncil.org/content-series/smart-partnerships/building-a-collaborative-ecosystem-for-ai-in-healthcare-in-low-and-middle-income-economies/>

In this article, the Atlantic Council's GeoTech Center discusses how over the past two decades AI has emerged as one of the most fundamental and widely adopted technologies of the Industrial Revolution 4.0. AI is poised to generate transformative and disruptive advances in healthcare through its unparalleled ability to translate large amounts of data into actionable insights for improving detection, diagnosis, and treatment of diseases; enhancing surveillance and accelerating public health responses; and now, for rapid drug discovery as well as interpretation of medical scans.

Given its range of applications, AI will undoubtedly play a central role in most nations' journeys toward Universal Health Coverage (UHC) and the United Nations Sustainable Development Goals (SDGs).<sup>260</sup> However, the development of AI for healthcare has been largely disparate<sup>261</sup> in low- and middle-income countries (LMICs) relative to high-income countries (HICs) even as their public health conditions are converging. As incomes have grown across the developing world, health outcomes and life expectancies in LMICs have markedly improved,<sup>262</sup> growing closer to those in HICs. This development has ignited a growing demand for services, rising costs of delivery and innovation, and challenges in building the appropriate workforce to deliver care.<sup>263</sup>

259 Abhinav Verma et al., "Building a collaborative ecosystem for AI in healthcare in Low and Middle Income Economies," Atlantic Council, August 27, 2020, accessed March 26, 2021, <https://www.atlanticcouncil.org/content-series/smart-partnerships/building-a-collaborative-ecosystem-for-ai-in-healthcare-in-low-and-middle-income-economies/>.

260 United Nations, *Report of the Secretary-General on SDG Progress 2019, Special Edition*, accessed March 26, 2021, [https://sustainabledevelopment.un.org/content/documents/24978Report\\_of\\_the\\_SG\\_on\\_SDG\\_Progress\\_2019.pdf](https://sustainabledevelopment.un.org/content/documents/24978Report_of_the_SG_on_SDG_Progress_2019.pdf).

261 Ahmed Hosny and Hugo J.W.L. Aerts, "Artificial intelligence for global health," *Science*, 366 (6468) (November 22, 2019): 955-956, DOI: 10.1126/science.aay5189, accessed March 26, 2021, <https://science.sciencemag.org/content/366/6468/955/tab-figures-data>

262 Esteban Ortiz-Ospina and Max Roser, "Global Health," *Our World in Data*, 2016, <https://ourworldindata.org/health-meta>.

263 McKinsey & Company, *Transforming healthcare with AI, The impact on the workforce and organisations*, March 2020, accessed March 26, 2021, [https://eithealth.eu/wp-content/uploads/2020/03/EIT-Health-and-McKinsey\\_Transforming-Healthcare-with-AI.pdf](https://eithealth.eu/wp-content/uploads/2020/03/EIT-Health-and-McKinsey_Transforming-Healthcare-with-AI.pdf).

This article concludes that:

- There is a large disparity in health outcomes in LMICs and HICs despite their having similar health conditions and incidents. This is evident in maternal mortality, under-five mortality, and instances of communicable disease. Many AI initiatives have been implemented to close this gap. AI is expected to help in the areas of access, safety, quality of care, efficiency, and education.
- These emerging transformations of healthcare technologies are most needed in LMICs. However, AI experimentation comes with complications because to support these initiatives it is imperative that a country has data availability, business model sustainability, and strong infrastructure, elements that may be in short supply in an LMIC. To counter this, the World Health Organization (WHO) produced a strategic plan for countries to prepare themselves for supporting eHealth systems. That plan includes policies, legislation, and standards.
- The best way to implement a functioning AI program is to start with data collection and management, and data sharing. Data privacy is a top concern in LMIC governments and stakeholders. As a result, it is recommended that regulations mandate and record all data to a set of standards. Open-source data banks, annotation tools, designated collaborative platforms, and peer reviews are the best way to achieve this.

#### **4. Western Society at the Crossroads, Part II: Smart Partnerships in a Changing World<sup>264</sup>**

Panelists: Mathew Burrows, director of the Atlantic Council's Foresight, Strategy, and Risks Initiative; Asha Jadeja Motwani, Founder, Motwani Jadeja Foundation; Julian Mueller-Kaler, resident fellow at the Atlantic Council's GeoTech Center and senior fellow at the Foresight, Strategy, and Risks Initiative; and Michael Schaefer, Chairman of the Board of Directors, BMW Foundation Herbert Quandt.

September 17, 2020

The recording is accessible at:

<https://www.atlanticcouncil.org/blogs/geotech-cues/event-recap-western-society-ii/>

As part of this event, panelists discussed how AI is rapidly becoming the next playing field for great-power competition between the United States and China. Worried about losing out, countries and state conglomerates around the world have begun pursuing

<sup>264</sup> GeoTech Center, "Event recap : Western society at the crossroads, part II: Smart partnerships in a changing world," Atlantic Council, September 16, 2020, accessed March 26, 2021, <https://www.atlanticcouncil.org/blogs/geotech-cues/event-recap-western-society-ii/>.

their own policy regimes and strive for digital sovereignty, but many express a hesitancy to pick sides.

Over the course of the past year, experts from the Atlantic Council's GeoTech Center organized meetings in Paris, Brussels, and Berlin; traveled to Beijing and Shanghai; and held virtual conferences with participants in India and Africa, while working to address two questions: What are the geopolitical implications of emerging technologies and how can countries build smart partnerships amid the widening gyre?

The event concluded that:

- Entrepreneurs are not focused on diplomatic relations between countries. Their priority is to make partnerships and profits for their company. Thus, nations could work with these companies in efforts to engage Asia in building partnerships involving data and AI.
- Nations can best encourage entrepreneurs to work together by accepting one another's cultural values and mindsets and by talking with each other, not about each other. By making an effort to be inclusive, nations and private enterprises are able to find common interests to keep technology business cooperative. Including Chinese leaders in this series of exchanges is an ideal next step to developing a positive business relationship.
- India, as a democracy and in close proximity to China, has attempted to play the role of broker between the United States and China. However, it has been difficult because of rising tensions and border clashes with China. India is now looking to play less of a role.
- Immigration is key when making sure that we do not widen the divide between nations. It is to the advantage of the United States to have international talent contributing in the country, so easing restrictions on immigration is beneficial. Additionally, encouraging US students to study in China helps build business relationships.

## 5. Transatlantic Cooperation in the Era of AI<sup>265</sup>

Panelists: Mircea Geoană, NATO deputy secretary general; Kim Jørgensen, head of Cabinet, Cabinet of Executive Vice-President Margrethe Vestager, European Commission; Eric Schmidt, chairman of the National Security Commission on Artificial Intelligence (NSCAI); and Robert O. Work, NSCAI vice chair.

265 Atlantic Council, "Transatlantic cooperation in the era of AI," Atlantic Council, October 28, 2020, accessed March 26, 2021, <https://www.atlanticcouncil.org/event/transatlantic-cooperation-in-the-era-of-ai/>.

October 28, 2020

The recording is accessible at:

<https://www.atlanticcouncil.org/event/transatlantic-cooperation-in-the-era-of-ai/>

Panelists discussed the future of the transatlantic relationship with respect to cooperation on artificial intelligence (AI), how best to promote shared values in the field, and what modern technologies mean in the defense and security context for European and US stakeholders.

In its Third Quarter Recommendations to the US Congress, the National Security Commission on Artificial Intelligence (NSCAI) proposed a Strategic Dialogue for Emerging Technologies (SDET) between the United States and the European Union. It encourages US policy makers to develop concrete actions to expand collaborative efforts and align transatlantic partners. In its March 2021 final report, NSCAI will build on these proposals to identify specific dialogue areas, which may include joint research and development (R&D) efforts and the development of privacy-enhancing AI applications, data sharing to facilitate cross-border projects, alignment of regulatory frameworks, coordinated investments in emerging technologies, facilitation of talent exchanges, and countering disinformation as well as intellectual property theft.

The event concluded that:

- The transatlantic relationship has produced extraordinary economic growth, military and national security, and cultural enrichment which has benefited citizens on both sides of the Atlantic. However, parties on both sides need to build a new partnership around AI since it is the most powerful tool in generations and all fundamental future accomplishments around science and engineering will have AI as a common denominator.
- Fostering a transatlantic talent ecosystem around AI, nurturing digital skills, and building a significant pool of “innovation champions” is a key priority. In line with the conclusions of NATO’s December 2019 summit in London and the European Commission’s “White Paper on Artificial Intelligence” released in February 2020, the transatlantic partner nations should build a road map for emerging disruptive technologies, including AI and big data, first-class connectivity, quantum computing, biotechnology, human enhancement, new materials, and space. In constructing this road map for emerging disruptive technologies, the partner nations should
  - Maintain a balance between traditional ways of deterrence and defense, while making a rapid and systematic transition to a new era of emerging technologies.

- Develop a balance between private and public initiatives and promote the transfer of best practices between government, private sector, and academia in order to accelerate innovation and discovery.
- Pursue all these initiatives by finding the common goals and interests across the North Atlantic community. At the same time, build respect for the existing differences of approach between a more regulatory environment in Europe and, in the United States, an ecosystem that gives preference to self-regulatory forces and that has a greater focus on defense-related issues.

## **6. Tech-Enabled Dis- and Misinformation, Social Platforms, and Geopolitics<sup>266</sup>**

Panelists: Pablo Breuer, nonresident fellow with the Atlantic Council's GeoTech Center and CISO of Helm Services; Rose Jackson, director of the Policy Initiative at the Atlantic Council's Digital Forensic Research Lab; and Sara-Jayne Terp, nonresident senior fellow with the Atlantic Council's GeoTech Center.

February 3, 2021

The recording is accessible at:

<https://www.atlanticcouncil.org/blogs/geotech-cues/event-recap-tech-enabled-dis-and-misinformation/>

As part of this event, the Atlantic Council's GeoTech Center and Digital Forensics Research Lab examined the influence of new technologies on dis- and misinformation via social media platforms, while discussing the various challenges caused by the era of the "free Internet" and social media's ability to provide a mass audience with unchecked, unregulated content.

Increased Internet access worldwide and the caveats on its expansion have helped propagate dis- and misinformation. In parallel, the lack of regulation of online communities and content creation has created massive echo chambers, shifting the way society operates. Due to this conflictive context, the public and federal lawmakers have put under scrutiny the role of free Internet and the growth of targeted advertisements in the social media business model. In particular, they are now questioning this model's financial incentives and its role in the expanding reach and harm caused by misinformation.

<sup>266</sup> Sana Moazzam, "Event recap | Tech-enabled dis- and misinformation, social platforms, and geopolitics," Atlantic Council, February 3, 2021, accessed March 26, 2021, <https://www.atlanticcouncil.org/blogs/geotech-cues/event-recap-tech-enabled-dis-and-misinformation/>.

Finally, panelists discussed the future of privacy and its newfound placement as a luxury product, where companies like Apple and ProtonMail have begun selling privacy and security as a feature to set themselves apart in an era of mass data collection.

The event concluded that:

- Social media users must be informed about how much of their data is actually collected and what it is used for.
- In Western nations, social media is treated much like the news media and should consequently be held to the same regulations that journalistic outlets are held to in order to ensure truthful information.
- In the relationships between privacy, democracy, and disinformation, increased security could drastically reduce content targeting, while there must be constructive efforts to combat disinformation by educating users, taking down botnets, and emphasizing transparency. In addition, acknowledging the presence of information deserts and working to eliminate them could prevent disinformation from filling the gap. Sophisticated techniques, such as utilizing advertisements in disinformation spaces to provide a diversified range of views, could also prove effective in altering radicalized echo chambers.
- There is a need to reestablish a US Information Agency through public-private partnership and create more applicable constraints and regulations. With technology rapidly improving and accelerating, achieving digital literacy is imperative for society. This would help the government get ahead of growing challenges and tackle its reputation for creating laws and regulating only after an incident has occurred.
- More broadly, although counter misinformation efforts are going in the right direction, they must, however, improve faster and continue to provide effective outcomes.

## Appendix F. Additional Readings

Marshall McLuhan, Quentin Fiore, and Shepard Fairey (Illustrator), *The Medium is the Message* (United Kingdom: Penguin Books, 1967).

Elinor Ostrom, *Governing the Commons: The Evolution of Institutions for Collective Action* (Cambridge University Press, 2015).

Yuval Noah Harari, *21 Lessons for the 21st Century* (United States: Spiegel & Grau; United Kingdom: Jonathan Cape, 2018).

Jared Diamond, *Guns, Germs and Steel: The Fate of Human Societies* (W. W. Norton & Company, 1997).

Annie Jacobsen, *The Pentagon's Brain: An Uncensored History of DARPA, America's Top-Secret Military Research Agency* (Little, Brown and Company, 2015).

Clifford Stoll, *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage* (Doubleday, 1989).

Kai-Fu Lee, *AI Superpowers: China, Silicon Valley, and the New World Order* (Houghton Mifflin Harcourt, 2018).

Mariana Mazzucato, *The Entrepreneurial State: Debunking Public vs. Private Sector Myths* (Anthem Press, 2013).

Richard A. Muller, *Physics for Future Presidents: The Science Behind the Headlines* (W. W. Norton & Company, 2008).

# Acronyms

---

<b>AI</b>	artificial intelligence
<b>APL</b>	Approved Product List
<b>AS</b>	autonomous system
<b>BGP</b>	Border Gateway Protocol
<b>CAIAC</b>	Collective and Augmented Intelligence Against COVID-19
<b>CARES Act</b>	Coronavirus Aid, Relief, and Economic Security Act
<b>CDC</b>	Centers for Disease Control and Prevention
<b>CDM</b>	Continuous Diagnostics and Mitigation
<b>CET</b>	critical and emerging technologies
<b>CEPI</b>	Coalition for Epidemic Preparedness Innovations
<b>CFIUS</b>	Committee on Foreign Investment in the United States
<b>CFO</b>	chief financial officer
<b>CHIPS Act</b>	Creating Helpful Incentives to Produce Semiconductors for America Act
<b>CIA</b>	Central Intelligence Agency
<b>CIO</b>	chief information officer
<b>CISA</b>	Cybersecurity and Infrastructure Security Agency
<b>CMMC</b>	Cybersecurity Maturity Model Certification
<b>COPUOS</b>	United Nations Committee on the Peaceful Uses of Outer Space
<b>CRISPR</b>	Clustered Regularly Interspaced Short Palindromic Repeats
<b>CUI</b>	controlled unclassified information
<b>DARPA</b>	Defense Advanced Research Projects Agency
<b>DCT</b>	digital contact tracing



<b>DHS</b>	Department of Homeland Security
<b>DISA</b>	Defense Information Systems Agency
<b>DoC</b>	Department of Commerce
<b>DoD</b>	Department of Defense
<b>DoDIN</b>	Department of Defense Information Network
<b>EIOS</b>	Epidemic Intelligence from Open Sources
<b>EO</b>	executive order
<b>EU</b>	European Union
<b>FASC</b>	Federal Acquisition Security Council
<b>FBI</b>	Federal Bureau of Investigation
<b>FCC</b>	Federal Communications Commission
<b>FDA</b>	Food and Drug Administration
<b>FedRAMP</b>	Federal Risk and Authorization Management Program
<b>FEMA</b>	Federal Emergency Management Agency
<b>FIMS</b>	federated identity management system
<b>FIPS</b>	Federal Information Processing Standards
<b>FIRRMA</b>	Foreign Investment Risk Review Modernization Act of 2018
<b>FISMA</b>	<i>Federal Information Security Modernization Act of 2014</i>
<b>GAO</b>	Government Accountability Office
<b>GDP</b>	gross domestic product
<b>GDPR</b>	General Data Protection Regulation
<b>GIS</b>	geographic information system
<b>GPAI</b>	Global Partnership on Artificial Intelligence
<b>GSA</b>	General Services Administration
<b>HHS</b>	Department of Health and Human Services

<b>HIC</b>	high-income countries
<b>HIPAA</b>	Health Insurance Portability and Accountability Act
<b>ICT</b>	<i>information and communications technology</i>
<b>IEC</b>	International Electrotechnical commission
<b>IHR</b>	International Health Regulations
<b>IP</b>	Internet Protocol
<b>IR</b>	international relations
<b>ISACs</b>	Information Sharing and Analysis Centers
<b>ISAO</b>	Information Sharing and Analysis Organizations
<b>ISO</b>	International Organization for Standardization
<b>IT</b>	information technology
<b>LEO</b>	low Earth orbit
<b>LMIC</b>	low- and middle-income countries
<b>LTS</b>	long term sustainability
<b>mRNA</b>	messenger RNA
<b>NAND</b>	(NOT-AND) is a logic gate
<b>NASA</b>	National Aeronautics and Space Administration
<b>NCATS</b>	National Cybersecurity Assessment and Technical Services
<b>NCEFOA</b>	National Center for Epidemic Forecasting and Outbreak Analytics
<b>NDAA</b>	National Defense Authorization Act
<b>NDN</b>	named data network, or named data networking
<b>NEON</b>	National Ecological Observatory Network
<b>NGA</b>	National Geospatial-Intelligence Agency
<b>NGO</b>	nongovernmental organization
<b>NICE</b>	National Initiative for Cybersecurity Education

<b>NIH</b>	National Institutes of Health
<b>NIST</b>	National Institute of Standards and Technology
<b>NSA</b>	National Security Agency
<b>NSCAI</b>	National Security Commission on Artificial Intelligence
<b>NSF</b>	National Science Foundation
<b>NSTC</b>	National Science and Technology Council
<b>NTIA</b>	National Telecommunications and Information Administration
<b>OMB</b>	Office of Management and Budget
<b>OST</b>	Outer Space Treaty
<b>OSTP</b>	Office of Science and Technology Policy
<b>OT</b>	operational technology
<b>PPD</b>	Presidential Policy Directive
<b>PPE</b>	personal protective equipment
<b>PPP</b>	public-private partnership
<b>PREDICT</b>	a project of USAID's Emerging Pandemic Threats program
<b>QC</b>	quantum cryptography
<b>QEDC</b>	Quantum Economic Development Consortium
<b>QIS</b>	quantum information science
<b>QKD</b>	quantum key distribution
<b>R&amp;D</b>	research and development
<b>S&amp;T</b>	science and technology
<b>SAGE</b>	Strategic Advisory Group of Experts on Immunization
<b>SAML</b>	Security Assertion Markup Language
<b>SBoM</b>	Software Bill of Materials
<b>SCRM</b>	supply chain risk management

<b>SDG</b>	Sustainable Development Goal
<b>STEM</b>	science, technology, engineering, and mathematics
<b>TCBMs</b>	transparency and confidence-building measures
<b>TS/SCI</b>	Top Secret/Sensitive Compartmented Information
<b>UHC</b>	Universal Health Coverage
<b>UK</b>	United Kingdom
<b>UN</b>	United Nations
<b>UNOOSA</b>	United Nations Office for Outer Space Affairs
<b>USAID</b>	United States Agency for International Development
<b>USDA</b>	United States Department of Agriculture
<b>USG</b>	United States government
<b>USMCA</b>	the United States-Mexico-Canada Free Trade Agreement
<b>VEP</b>	Vulnerabilities Equities Process
<b>WHO</b>	World Health Organization

# Biographies of the GeoTech Commission Co-Chairs and Commissioners

## Co-chairs

### **John Goodman, Chief Executive Officer, Accenture Federal Services**

John Goodman is the Chief Executive of Accenture Federal Services (AFS), which serves clients across all sectors of the US federal government - defense, intelligence, public safety, health, and civilian. Since joining Accenture in 1998, he has held a variety of leadership roles - including managing director of Accenture's Defense & Intelligence portfolio, head of Management Consulting for the global Public Service Operating Group, and most recently Chief Operating Officer of AFS. John began his career at Accenture as a Member of the Communications & High Technology practice.

Prior to joining Accenture, John served for five years in the federal government as Deputy Under Secretary of Defense (Industrial Affairs & Installations), Deputy Assistant Secretary of Defense (Industrial Affairs), and a member of the staff of the National Economic Council, the White House office responsible for coordination of economic policy. He previously served on the Harvard Business School faculty.

John is co-chair of the Atlantic Council's GeoTech Commission and member of the boards of both the Atlantic Council and the Northern Virginia Technology Council, as well as a member of the Council on Foreign Relations. He is a member, and the immediate past chair, of the Executive Committee of the Professional Services Council, a former member of the Executive Committee of AFCEA, and the former chairman of the Defense Business Board. John was named Executive of the Year by the Greater Washington Government Contractors in 2018; a Wash100 inductee in 2018, 2019, 2020 and 2021; and a Fed100 Award winner in 2015. He has been awarded the Office of the Secretary of Defense Medal for Exceptional Public Service, the Department of Defense Medal for Distinguished Public Service, and the Department of Defense Medal for Outstanding Public Service.

John received his Bachelor of Arts, summa cum laude, from Middlebury College and his Master of Arts and Ph.D. from Harvard University.

### **Teresa Carlson, President and Chief Growth Officer, Splunk**

As President and Chief Growth Officer at Splunk, Teresa Carlson leads our efforts to align and drive our ongoing business transformations across Splunk's go-to-market segments. Most recently, Carlson served as Vice President, Worldwide Public Sector and Industries, for Amazon Web Services (AWS). After she founded AWS's Worldwide Public Sector in 2010, Carlson's role eventually expanded to include financial services, energy services, telecommunications, and aerospace and services industry business units.

Carlson has also been a strong advocate for empowering women in the technology field. That passion led to the creation of "We Power Tech," AWS's diversity and inclusion initiative, which aims to ensure underrepresented groups – including women – are reflected throughout all AWS outreach efforts. Carlson dedicates time to philanthropic and leadership roles in support of the global community. Prior to joining AWS in 2010, Carlson led sales, marketing and business development organizations at Microsoft, Keyfile/Lexign and NovaCare. Carlson holds a B.A. and M.S. from Western Kentucky University.

### **Honorary Co-Chairs**

#### **Mark R. Warner, U.S. Senator from Virginia**

Senator Warner was elected to the U.S. Senate in November 2008 and reelected to a third term in November 2020. He serves on the Senate Finance, Banking, Budget, and Rules Committees as well as the Select Committee on Intelligence, where he is the Chairman. During his time in the Senate, Senator Warner has established himself as a bipartisan leader who has worked with Republicans and Democrats alike to cut red tape, increase government performance and accountability, and promote private sector innovation and job creation. Senator Warner has been recognized as a national leader in fighting for our military men and women and veterans, and in working to find bipartisan, balanced solutions to address our country's debt and deficit.

From 2002 to 2006, he served as Governor of Virginia. When he left office in 2006, Virginia was ranked as the best state for business, the best managed state, and the best state in which to receive a public education.

The first in his family to graduate from college, Mark Warner spent 20 years as a successful technology and business leader in Virginia before entering public office. An early investor in the cellular telephone business, he co-founded the company that became Nextel and invested in hundreds of start-up technology companies that created tens of thousands of jobs.

Senator Warner and his wife Lisa Collis live in Alexandria, Virginia. They have three daughters.

#### **Rob Portman, U.S. Senator for Ohio**

Rob Portman is a United States Senator from the state of Ohio, a position he has held since he was first elected in 2010. Portman previously served as a U.S. Representative, the 14th United States Trade Representative, and the 35th Director of the Office of Management and Budget (OMB). In 1993, Portman won a special election to represent Ohio's 2nd congressional district in the U.S. House of Representatives and served six terms before President George W. Bush appointed him as U.S. Trade Representative in May 2005. Portman currently serves as the Ranking Member on the Senate Homeland Security and Governmental Affairs Committee, as well as on the Senate Finance and Foreign Relations Committees. He was born and raised in Cincinnati, where he still lives today with his wife Jane. Together they have three children: Jed, Will, and Sally.

#### **Suzan DelBene, U.S. Congresswoman Representing Washington's 1st District**

Congresswoman Suzan DelBene represents Washington's 1st Congressional District, which spans from northeast King County to the Canadian border and includes parts of King, Snohomish, Skagit, and Whatcom counties. First sworn into the House of Representatives in November 2012, Suzan brings a unique voice to the nation's capital with more than two decades of experience as a successful technology entrepreneur and business leader. Suzan takes on a wide range of challenges both in Congress and in the 1st District and is a leader on issues of technology, health care, trade, taxes, environmental conservation, and agriculture.

Suzan currently serves as the Vice Chair on the House Ways and Means Committee, which is at the forefront of debate on a fairer tax code, health care reform, trade deals, and lasting retirement security. She serves on the Select Revenue Measures and Trade Subcommittees. Suzan also serves as Chair of the forward-thinking New Democrat Coalition, which is one of the largest ideological coalitions in the House, and is co-chair of the Women's High Tech Caucus, Internet of Things Caucus, and Dairy Caucus. She is also a member of the Pro-Choice Caucus.

Over more than two decades as an executive and entrepreneur, she helped to start drugstore.com as Vice President of Marketing and Store Development, and served as CEO and President of Nimble Technology, a business software company based on technology developed at the University of Washington. Suzan also spent 12 years at Microsoft, most recently as corporate vice president of the company's mobile communications business.

Before being elected to Congress, Suzan served as Director of the Washington State Department of Revenue. During her tenure, she proposed reforms to cut red tape for small businesses. She also enacted an innovative tax amnesty program that generated \$345 million to help close the state's budget gap while easing the burden on small businesses.

Suzan and her husband, Kurt DelBene, have two children, Becca and Zach, and a dog named Reily.

### **Michael T. McCaul, U.S. Congressman Representing Texas' 10th District**

Congressman Michael T. McCaul is currently serving his ninth term representing Texas' 10th District in the United States Congress. The 10th Congressional District of Texas stretches from the city of Austin to the Houston suburbs and includes Austin, Bastrop, Colorado, Fayette, Harris, Lee, Travis, Washington and Waller Counties.

At the start of the 116th Congress, Congressman McCaul became the Republican Leader of the *Foreign Affairs* Committee. This committee considers legislation that impacts the diplomatic community, which includes the Department of State, the Agency for International Development (USAID), the Peace Corps, the United Nations, and the enforcement of the Arms Export Control Act. In his capacity as the committee's Republican Leader, McCaul is committed to ensuring we promote America's leadership on the global stage. In his view, it is essential the United States bolsters international engagement with our allies, counters the aggressive policies of our adversaries, and advances the common interests of nations in defense of stability and democracy around the globe. He will continue to use his national security expertise to work to counter threats facing the United States, especially the increasing threat we face from nation state actors such as China, Iran, Russia, North Korea, among others.

Prior to Congress, Michael McCaul served as Chief of Counter Terrorism and National Security in the U.S. Attorney's office, Western District of Texas, and led the Joint Terrorism Task Force charged with detecting, deterring, and preventing terrorist activity. McCaul also served as Texas Deputy Attorney General under current U.S. Senator John Cornyn, and served as a federal prosecutor in the Department of Justice's Public Integrity Section in Washington, DC.

A fourth generation Texan, Congressman McCaul earned a B.A. in Business and History from Trinity University and holds a J.D. from St. Mary's University School of Law. In 2009 Congressman McCaul was honored with St. Mary's Distinguished Graduate award. He is also a graduate of the Senior Executive Fellows Program of the School of Government, Harvard University. Congressman McCaul is married to his wife, Linda. They are proud parents of five children: Caroline, Jewell, and the triplets Lauren, Michael, and Avery.



## **Commissioners**

### **Max R. Peterson II, Vice President, Worldwide Public Sector, Amazon Web Services**

Max Peterson is Vice President for Amazon Web Services' (AWS) Worldwide Public Sector. In this role, Max supports public sector organizations as they leverage the unique advantages of commercial cloud to drive innovation among government, educational institutions, health care institutions, and nonprofits around the world.

A public sector industry veteran with thirty years of experience, he has an extensive background in developing relationships with public sector customers. He has previously worked with Dell Inc. as Vice President and General Manager for Dell Federal Civilian and Intelligence Agencies, as well as CDWG and Commerce One.

Max earned both a Bachelor's Degree in Finance and Master's of Business Administration in Management Information Systems from the University of Maryland.

### **Paul Daugherty, Accenture Chief Executive – Technology and Chief Technology Officer**

Paul Daugherty is Accenture's Group Chief Executive – Technology & Chief Technology Officer. He leads all aspects of Accenture's technology business. Paul is also responsible for Accenture's technology strategy, driving innovation through R&D in Accenture Labs and leveraging emerging technologies to bring the newest innovations to clients globally. He recently launched Accenture's Cloud First initiative to further scale the company's market-leading cloud business and is responsible for incubating new businesses such as blockchain, extended reality and quantum computing. He founded and oversees Accenture Ventures, which is focused on strategic equity investments and open innovation to accelerate growth. Paul is responsible for managing Accenture's alliances, partnerships and senior-level relationships with leading and emerging technology companies, and he leads Accenture's Global CIO Council and annual CIO and Innovation Forum. He is a member of Accenture's Global Management Committee.

### **Maurice Sonnenberg, Guggenheim Securities**

Maurice Sonnenberg has served as an outside advisor to five Presidential Administrations in the areas of international trade, finance, international relations, intelligence, and foreign election monitoring. In 1994 and 1995, he served as a member of the US Commission on Protecting and Reducing Government Secrecy, and from 1996 as the Senior Advisor to the US Commission on the Roles and Capabilities of the US Intelligence Community. He was a member of the President's Foreign Intelligence Advisory Board under President Bill Clinton for 8 years. In 2002, he was a member of the Task

Force of Terrorist Financing for the Council on Foreign Relations. From 2007-2010, he served on the Department of Homeland Security Advisory Council and the Panel Advisory Board for the Secretary of the Navy from 2008-2015. In 2012-14, he served as co-Chairman of the National Commission for the Review of the Research and Development Programs for the Intelligence Community. He has also served as an Official US Observer at elections in Latin America. This includes multiple elections in El Salvador, Guatemala, Nicaragua and Mexico. Sonnenberg has worked at the investment banking firms Donaldson Lufkin and Jenrette, Bear Stearns, and J.P. Morgan, and at the law firms Hunton & Williams, Manatt, Phelps & Phillips. Currently, he is with Guggenheim Securities as Senior International Advisor. He is also a Senior Advisor to the Advanced Metallurgical Group, N.V.

#### **Michael Chertoff, Former U.S. Secretary of Homeland Security**

Michael Chertoff is the Executive Chairman and Co-Founder of The Chertoff Group. From 2005 to 2009, he served as Secretary of the U.S. Department of Homeland Security. Earlier in his career, Mr. Chertoff served as a federal judge on the U.S. Court of Appeals for the Third Circuit and head of the U.S. Department of Justice's Criminal Division. He is the Chairman of the Board of Directors of BAE Systems, Inc., the U.S.-based subsidiary of BAE Systems plc. In 2018, he was named the chairman of the Board of Trustees for Freedom House. He currently serves on the board of directors of Noblis and Edgewood Networks. In the last five years, Mr. Chertoff co-chaired the Global Commission in Stability of Cyberspace and also co-chairs the Transatlantic Commission on Election Integrity. Chertoff is magna cum laude graduate of Harvard College and Harvard Law School.

#### **Michael J. Rogers, Former Chairman of the U.S. House Permanent Select Committee on Intelligence**

Mike Rogers is a former member of Congress, where he represented Michigan's Eighth Congressional District for seven terms. While in the U.S. House of Representatives, he chaired the powerful House Permanent Select Committee on Intelligence (HPSCI), authorizing and overseeing a budget of \$70 billion that funded the nation's seventeen intelligence agencies. Mr. Rogers built a legacy as a bipartisan leader on cybersecurity, counterterrorism, intelligence, and national security policy. Mr. Rogers worked with two presidents, congressional leadership, and countless foreign leaders, diplomats, and intelligence professionals. Before joining Congress, he served as an officer in the US Army and as a Special Agent with the FBI. He is currently investing in and helping build companies that are developing solutions for healthcare, energy efficiency, and communications challenges. He also serves as a regular national security commentator on CNN and hosted the channel's documentary-style original series *Declassified*.

Mr. Rogers is a regular public speaker on global affairs, cybersecurity, and leadership. He is married to Kristi Rogers and has two children.

**Pascal Marmier, Head, Economy of Trust Foundation, SICPA**

Pascal Marmier is head of SICPA's Economy of Trust Foundation. Most recently, Marmier held several positions in the United States within Swiss Re, a global reinsurer, focusing on digital strategy and innovation management. Previously, he spent twenty years as a Swiss diplomat as one of the early leaders of the Swissnex network, a private-public partnership dedicated to facilitating collaboration with Swiss universities, startups, and corporations in all fields related to science, technology, and innovation. After spending a decade establishing key partnerships and activities in Boston, Marmier moved to China to establish the Swissnex platform in the region. He holds law degrees from the University of Lausanne and Boston University, as well as an MBA from the MIT Sloan School of Management.

**Ramayya Krishnan, PhD, Director, Block Center for Technology and Society, Carnegie Mellon University**

Ramayya Krishnan is the W. W. Cooper and Ruth F. Cooper Professor of Management Science and Information Systems at Carnegie Mellon University. He is Dean of the H. John Heinz III College of Information Systems and Public Policy and directs the Block Center for Technology and Society at the university. His scholarly contributions have focused on mathematical modeling of organizational decision making, the design of data driven decision support systems and statistical models of consumer behavior in digital environments. He advises governments, businesses and development banks on digital transformation technology and its consequences.

**Dr. Shirley Ann Jackson, President, Rensselaer Polytechnic Institute**

The Honorable Shirley Ann Jackson, Ph.D., has served as the 18th president of Rensselaer Polytechnic Institute since 1999. A theoretical physicist described by Time Magazine as “perhaps the ultimate role model for women in science,” Dr. Jackson has held senior leadership positions in academia, government, industry, and research. She is the recipient of many national and international awards, including the National Medal of Science, the United States’ highest honor for achievement in science and engineering. Dr. Jackson served as Co-Chair of the United States President’s Intelligence Advisory Board from 2014 to 2017 and as a member of the President’s Council of Advisors on Science and Technology from 2009 to 2014. Before taking the helm at Rensselaer, she was Chairman of the U.S. Nuclear Regulatory Commission from 1995 to 1999. She serves on the boards of major corporations that include FedEx and PSEG, where she is Lead Director.

Dr. Jackson holds an S.B. in Physics, and a Ph.D. in Theoretical Elementary Particle Physics, both from MIT.

**Susan M. Gordon, Former Principal Deputy Director of National Intelligence**

The Honorable Susan (Sue) M. Gordon served as Principal Deputy Director of National Intelligence from August 2017 until August 2019. In her more than three decades of experience in the IC, Ms. Gordon served in a variety of leadership roles spanning numerous intelligence organizations and disciplines, including serving as the Deputy Director of the National Geospatial-Intelligence Agency (NGA) from 2015 to 2017. In this role, she drove NGA's transformation to meet the challenges of a 21st century intelligence agency. Since leaving government service, Ms. Gordon serves on a variety of public and private boards, is a fellow at Duke and Harvard Universities, and consults with a variety of companies on technology—including cyber and space—strategy, and leadership, focusing on shared responsibility for national and global security.

**Vint Cerf**

Vinton G. Cerf is vice president and Chief Internet Evangelist for Google. Cerf is the codesigner of the TCP/IP protocols and the architecture of the Internet. He has served in executive positions at the Internet Corporation for Assigned Names and Numbers, the Internet Society, MCI, the Corporation for National Research Initiatives, and the Defense Advanced Research Projects Agency. A former Stanford Professor and member of the National Science Board, he is also the past president of the Association for Computing Machinery and serves in advisory capacities at the National Institute of Standards and Technology, the Department of Energy, and the National Aeronautics and Space Administration. Cerf is a recipient of numerous awards for his work, including the US Presidential Medal of Freedom, US National Medal of Technology, the Queen Elizabeth Prize for Engineering, the Prince of Asturias Award, the Tunisian National Medal of Science, the Japan Prize, the Charles Stark Draper Prize, the ACM Turing Award, the Legion d'Honneur, the Franklin Medal, Foreign Member of the British Royal Society and Swedish Academy of Engineering, and twenty-nine honorary degrees. He is a member of the Worshipful Company of Information Technologists and the Worshipful Company of Stationers.

**Zia Khan, PhD, Vice President for Innovation, The Rockefeller Foundation**

As Senior Vice President for Innovation, Zia Khan oversees the Rockefeller Foundation's approach to developing solutions that can have a transformative impact on people's lives through the use of convenings, data and technology, and strategic partnerships. He writes and speaks frequently on leadership, strategy, and innovation. Khan has served on the World Economic Forum Advisory Council for Social Innovation and the

US National Advisory Board for Impact Investing. He leads a range of the Rockefeller Foundation's work in applying data science for social impact and ensuring artificial intelligence contributes to an inclusive and equitable future.

Prior to joining the Rockefeller Foundation, Khan was a management consultant advising leaders in technology, mobility, and private equity sectors. He worked with Jon Katzenbach on research related to leadership, strategy, and organizational performance, leading to their book, *Leading Outside the Lines*.

Zia holds a BS from Cornell University and MS and PhD from Stanford University.

**Anthony Scriffignano, PhD, Senior Vice President, Chief Data Scientist at Dun & Bradstreet Corporation**

Anthony Scriffignano, PhD is Senior Vice President, Chief Data Scientist at Dun & Bradstreet Corporation. He is an internationally recognized data scientist with experience spanning over forty years in multiple industries and enterprise domains. Scriffignano has extensive background in advanced anomaly detection, computational linguistics and advanced inferential algorithms, leveraging that background as primary inventor on multiple patents worldwide. Scriffignano was recognized as the U.S. Chief Data Officer of the Year 2018 by the CDO Club, the world's largest community of C-suite digital and data leaders. He is also a member of the OECD Network of Experts on AI working group on implementing Trustworthy AI, focused on benefiting people and the planet. He has briefed the US National Security Telecommunications Advisory Committee and contributed to three separate reports to the president, on Big Data Analytics, Emerging Technologies Strategic Vision, and Internet and Communications Resilience. Additionally, Scriffignano provided expert advice on private sector data officers to a group of state Chief Data Officers and the White House Office of Science and Technology Policy. Scriffignano serves on various advisory committees in government, private sector, and academia. Most recently, he has been called upon to provide insight on data science implications in the context of a highly disrupted datasphere and the implications of the global pandemic. He is considered an expert on emerging trends in advanced analytics, the "Big Data" explosion, artificial intelligence, multilingual challenges in business identity and malfeasance in commercial and public-sector contexts.

**Frances F. Townsend, Executive Vice President, Activision Blizzard**

Frances Fragos Townsend is the Executive Vice President of Corporate Affairs, Chief Compliance Officer and Corporate Secretary at Activision Blizzard. Prior to that, she was Vice Chairman, General Counsel and Chief Administration Officer at MacAndrews & Forbes, Inc. In her 10 years there, she focused internally on financial, legal and personnel issues, as well as international, compliance and business development across

MacAndrews' portfolio companies. Prior to that, she was a corporate partner with the law firm of Baker Botts, LLP. From 2004 to 2008, Ms. Townsend served as Assistant to President George W. Bush for Homeland Security and Counterterrorism and chaired the Homeland Security Council. She also served as Deputy National Security Advisor for Combatting Terrorism from 2003 to 2004. Ms. Townsend spent 13 years at the US Department of Justice under the administrations of President George H. W. Bush, President Bill Clinton and President George W. Bush. She has received numerous awards for her public service accomplishments. Ms. Townsend is a Director on the Board of two public companies: Chubb and Freeport McMoRan. She previously served on the Boards at Scientific Games, SciPlay, SIGA and Western Union. She is an on-air senior national security analyst for CBS News. Ms. Townsend previously served on the Director of National Intelligence's Senior Advisory Group, the Central Intelligence Agency's (CIA) External Advisory Board and the US President's Intelligence Advisory Board. Ms. Townsend is a trustee on the Board of the New York City Police Foundation, the Intrepid Sea, Air & Space Museum, the McCain Institute, the Center for Strategic and International Studies (CSIS) and the Atlantic Council. She also serves on the Board at the Council on Foreign Relations, on the Executive Committee of the Trilateral Commission and the Board of the International Republican Institute. She is a member of the Aspen Strategy Group.

**Admiral James Stavridis, USN, Ret.**

Admiral James Stavridis is an Operating Executive of The Carlyle Group and Chair of the Board of Counselors of McLarty Global Associates, following five years as the 12th Dean of The Fletcher School of Law and Diplomacy at Tufts University. He also serves as the Chairman of the Board of the Rockefeller Foundation. A retired four-star officer in the U.S. Navy, he led the North Atlantic Treaty Organization (NATO) Alliance in global operations from 2009 to 2013 as Supreme Allied Commander with responsibility for Afghanistan, Libya, the Balkans, Syria, counter piracy and cyber security. He also served as Commander of U.S. Southern Command, with responsibility for all military operations in Latin America from 2006 to 2009. He earned more than 50 medals, including 28 from foreign nations in his 37-year military career. Admiral Stavridis earned a PhD in international relations and has published 10 books and hundreds of articles in leading journals around the world, including the recent novel "2034: A Novel of the Next World War," which was a *New York Times* bestseller. His 2012 TED Talk on global security has close to one million views. Admiral Stavridis is a monthly columnist for TIME Magazine and Chief International Security Analyst for NBC News.

# Biographies of Supporting Atlantic Council Staff

## **Dr. David A. Bray, Director, GeoTech Center, Atlantic Council**

Dr. David A. Bray has served in a variety of leadership roles in turbulent environments, including bioterrorism preparedness and response from 2000 to 2005, time on the ground in Afghanistan in 2009, serving as a non-partisan Senior National Intelligence Service Executive directing a bipartisan National Commission for the Review of the Research and Development Programs of the US Intelligence Community, and providing leadership as a non-partisan federal agency Senior Executive where he led a team that received the global CIO 100 Award twice in 2015 and 2017. He is an Eisenhower Fellow, Marshall Memorial Fellow, and Senior Fellow with the Institute for Human & Machine Cognition. *Business Insider* named him one of the top “24 Americans Who Are Changing the World” and the World Economic Forum named him a Young Global Leader. Over his career, he has advised six different start-ups, led an interagency team spanning sixteen different agencies that received the National Intelligence Meritorious Unit Citation, and received the Joint Civilian Service Commendation Award, the National Intelligence Exceptional Achievement Medal, Arthur S. Flemming Award, as well as the Roger W. Jones Award for Executive Leadership. He is the author of more than forty academic publications, was invited to give the AI World Society Distinguished Lecture to the United Nations in 2019, and was named by HMG Strategy as one of the Global “Executives Who Matter” in 2020.

## **Dr. Peter Brooks, Consultant, GeoTech Center, Atlantic Council**

Peter Brooks is a senior researcher and national security analyst at the Institute for Defense Analyses, a federally funded research and development center. For more than three decades, he has contributed to the understanding of critical national security issues for a wide range of government agencies. His broad expertise includes intelligence analysis, advanced technologies and applications, and joint force analyses, experimentation, strategy, and cost assessments.



**Stephanie Wander, Deputy Director, GeoTech Center, Atlantic Council**

Stephanie Wander is a technology and innovation strategist with a successful track record of launching large-scale projects to solve global grand challenges. Ms. Wander's approaches integrate innovation best practices and mindsets, including design thinking, behavior change strategies, foresight techniques, and expert and public crowdsourcing.

Previously, Ms. Wander was a lecturer at the University of Southern California Suzanne Dworak-Peck School of Social Work where she taught graduate social work professionals in design, innovation, and disruptive technology.

**Rose Butchart, Senior Adviser, National Security Initiatives, GeoTech Center, Atlantic Council**

Rose Butchart is the senior adviser for National Security Initiatives at the Atlantic Council's GeoTech Center.

As a program manager for the Department of Defense's National Security Innovation Network, she managed, designed, and scaled a variety of programs, including a technology, transfer, and transition (T3) program designed to bring breakthrough Department of Defense lab technology to market—and to the warfighter. She also managed a workshop series to tackle some of the military's intractable problems and a fellowship which placed active duty military and Department of Defense civilians at technology start-ups.

**Claudia Vaughn Zittle, Program Assistant, Atlantic Council GeoTech Center**

Claudia Vaughn Zittle was a program assistant with the Atlantic Council's GeoTech Center. In this role, she managed a wide range of projects at the intersection of emerging technologies and dynamic geopolitical landscapes. She also conducted research and provided written analysis for publication on Atlantic Council platforms.

Originally from the Washington, DC, area, she received her BA in International Relations from Cornell College. She is continuing her education at American University's School of International Service, where she studies International Relations with a concentration in US Foreign Policy and National Security.

**Claire Branley, Program Assistant, Atlantic Council GeoTech Center**

Claire Branley joined the Atlantic Council's Geotech Center after graduating from the University of Washington with a BS in Public Health and Global Health. She was a research assistant in the Moussavi-Harami Lab, uncovering gene therapies for inherited heart disease. She is deeply passionate about the prevention of disease and has assisted several maternal and child health research projects and volunteered in farm-to-food pantry initiatives to decrease food insecurity in the Seattle area. Her interests include chronic disease burden, global food security, and promoting interdisciplinary solutions.

# Biographies of the Key Contributors to the GeoTech Commission Report

## Research and writing on misinformation

### **Dr. Pablo Breuer, Nonresident Senior Fellow, GeoTech Center, Atlantic Council**

Dr. Pablo Breuer is an information/cyber warfare expert and a twenty-two-year veteran of the US Navy with tours including the National Security Agency, US Cyber Command, and United States Special Operations Command. He is a cofounder of the Cognitive Security Collaborative and coauthor of the Adversarial Misinformation and Influence Tactics and Techniques (AMITT) framework.

### **Dr. Robert Leonhard, National Security Analysis, Johns Hopkins University Applied Physics Laboratory**

Robert Leonhard is on the principal professional staff as an analyst in the National Security Analysis Department of Johns Hopkins University's Applied Physics Laboratory (JHU/APL). His main areas of focus are irregular warfare, nuclear deterrence, and game design. Prior to joining JHU/APL, he earned a PhD in American History from West Virginia University, a Master of Military Arts and Sciences from the US Army, an MS in International Relations from Troy State University, and a BS in European History from Columbus University. He is a retired Army infantry officer and planner. He is the author of *The Art of Maneuver* (Presidio Press, 1991), *Fighting by Minutes: Time and the Art of War* (Praeger, 1994), *The Principles of War for the Information Age* (Presidio Press, 1998), *Little Green Men: a primer in Russian Unconventional Warfare, Ukraine 2013-2014* (JHUAPL, 2016), and *The Defense of Battle Position Duffer: Cyber-Enabled Maneuver in Multi-Domain Battle* (JHUAPL, 2016). He may be contacted at Robert.L Leonhard@jhuapl.edu.

### **John Renda, Program Manager, Army Special Operations, Johns Hopkins University Applied Physics Laboratory**

Col. John Renda, USA (Ret), is a program manager for Army Special Operations at the Johns Hopkins University's Applied Physics Laboratory. He graduated from Tulane University with a degree in Political Science and International Relations, and earned a MS in

National Security from the US Naval War College. He served as a career Psychological Operations officer in US Army Special Operations. His key assignments included 75th Ranger Regiment Information Operations Officer, 1st Psychological Operations Battalion Commander, United States Special Operations Command (USSOCOM) Director J39 National Capital Region, and National Security Council Staff, Director for Strategic Communication. He may be contacted at [john.renda@jhuapl.edu](mailto:john.renda@jhuapl.edu).

**Dr. Sara-Jayne Terp, Nonresident Senior Fellow, GeoTech Center, Atlantic Council**

Sara-Jayne Terp builds frameworks to improve how autonomous systems, algorithms, and human communities work together. At Threet Consulting, she creates processes and technologies to support community-led disinformation defence. She is an Atlantic Council Senior Fellow, CogSecCollab lead, and chair at CAMLIS and Defcon AI Village. Her background includes intelligence systems, crowdsourced data gathering, autonomous systems (e.g., human-machine teaming), data strategy, data ethics, policy, nation state development, and crisis response.

**Appendix B**

**Stewart Scott, Assistant Director, GeoTech Center, Atlantic Council**

Stewart Scott is an assistant director with the Atlantic Council's GeoTech Center, where he conducts research and provides written analysis for publication on Atlantic Council platforms and works on joint projects with other centers in the Atlantic Council. He earned his AB, along with a minor in Computer Science, at the School of Public and International Affairs at Princeton University.

We would also like to thank the following members of the Atlantic Council's Cyber Statecraft Initiative for their contributions to Appendix B: **Trey Herr, Simon Handler, Madison Lockett, Will Loomis, Emma Schroeder, and Tianjiu Zuo.**

**Appendix C and writings on global health**

**Dr. Divya Chander, Nonresident Senior Fellow, GeoTech Center, Atlantic Council**

Divya Chander, MD, PhD is a physician-scientist, futurist, and entrepreneur (co-founder of 2 startups). She is a practicing anesthesiologist with specializations in neurosurgery, ENT, and critical care. As a data scientist with expertise in neural signal processing, she has developed algorithms to automate tracking of states of consciousness. Dr. Chander is also Chair of Neuroscience at Singularity University, a Silicon Valley think tank for data and technology acceleration, applications, and ethics. She serves as medical, science, and technology advisor to a number of companies in the medical, space life

sciences, and neurotechnology spaces. Dr. Chander was named one of 2020's top digital health innovators by Intelligent Health AI. As Nonresident Senior Fellow at the Geotech Center, she collaborates to foster good data and technology policy choices for key stakeholders around the world in the area of data trusts, data security, public health, and pandemic resilience.

## **Appendix D**

### **Inkoo Kang, Research Consultant, GeoTech Center, Atlantic Council**

US Air Force 2<sup>nd</sup> Lt. Inkoo Kang is a research consultant for the Atlantic Council's GeoTech Center. At the Atlantic Council, he conducts research and provides written analyses on the increasingly important role of outer space for social, economic, and military operations. His main interest focuses on how emerging technologies are merging military, diplomatic, humanitarian, and economic challenges and how the military must learn to adapt to such threats.

## **Appendix E**

### **Borja Prado, Research Assistant, GeoTech Center Atlantic Council**

Borja Prado holds an MS in Foreign Service (MSFS) from Georgetown University, where he concentrated in Global Politics and Security, focusing on the impact of disruptive technologies on governments, businesses, and societies.

He aims to apply his research experience, language skills, and strong background in technology and global affairs to help governments, businesses, and societies succeed in this increasingly uncertain era.

# Acknowledgements

---

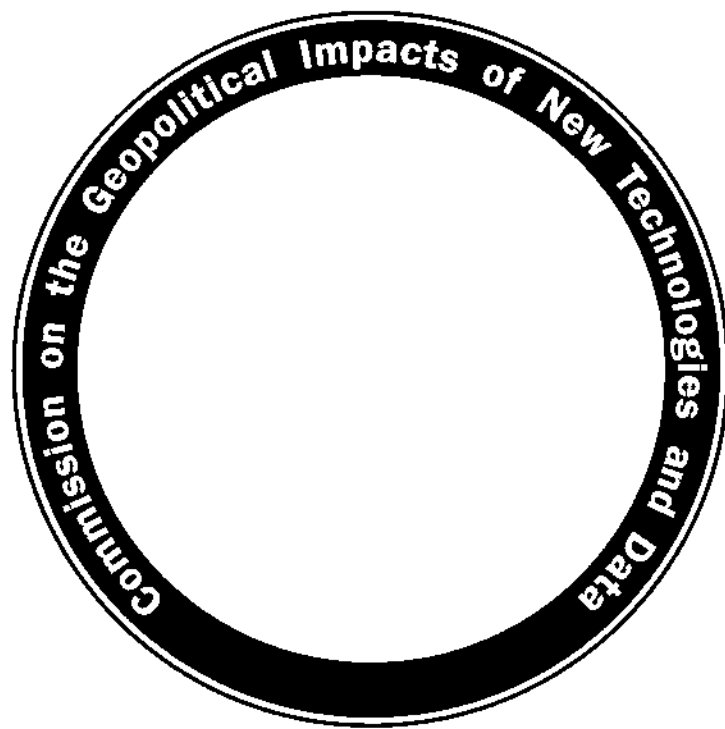
We would like to thank the following members of the Commission Co-Chair teams for their assistance, expertise, and technical review of the report:

- **Stoney Burke**, Head of Federal Affairs and Public Policy, Amazon Web Services
- **Ira Entis**, Managing Director, Growth and Strategy Lead, Accenture Federal Services
- **Geoffrey Kahn**, Managing Director, Government Relations, Accenture
- **Pamela Merritt**, Managing Director, Federal Marketing and Communications, Accenture Federal Services
- **Davis Pace**, Professional Staff Member, House *Foreign Affairs* Committee
- **Sean Sweeney**, Manager, Government Relations, Accenture
- **Clayton Swope**, Senior Manager, National Security Public Policy, Amazon Web Services
- **Carolyn Vigil**, Senior Customer Engagement Manager, Amazon Web Services

We would like to acknowledge the following individuals for their review and commentary on relevant sections of the report: **Laura Bate, Natalie Barrett, Pablo Breuer, Mark Brunner, Mung Chiang, Kevin Clark, Donald Codling, Carol Dumaine, Ryan G. Faith, Melissa Flagg, James F. Geurts, Jasper Gilardi, Bob Gourley, Bob Greenberg, Simon Handler, Henry Hertzfeld, Robert Hoffman, Erich James Hösli, Diane M. Janosek, William Jeffrey, Charles Jennings, Declan Kirrane, John J. Klein, Sandra J. Laney, John Logsdon, Robert Lucas, Lauren Maffeo, Jerry Mechling, Ivan Medynskyi, Ben King, Ben Murphy and the team at Reaching the Future Faster LLC, James Olds, Nikhil Raghuveera, Matthew Rose, Benjamin Schatz, Emma Schroeder, Jeremy Spaulding, Keith Strier, Daniella Taveau, Trent Teyema, Bill Valdez, and Tiffany Vora.**

We also would like to express sincere appreciation to individuals both internal and external to the Atlantic Council for help in preparing this report for final publication. Their professional and dedicated efforts were essential to this work.

Lastly, we want to thank all the GeoTech Fellows and GeoTech Action Council members, each of whom embodies the spirit of the new Center as we look to the future ahead: **Be Bold. Be Brave. Be Benevolent.**





# Atlantic Council

## Board of Directors

### CHAIRMAN

\*John F.W. Rogers

### EXECUTIVE

### CHAIRMAN

### EMERITUS

\*James L. Jones

### PRESIDENT AND CEO

\*Frederick Kempe

### EXECUTIVE VICE

### CHAIRS

\*Adrienne Arsht

\*Stephen J. Hadley

### VICE CHAIRS

\*Robert J. Abernethy

\*Richard W. Edelman

\*C. Boyden Gray

\*Alexander V. Mirtchev

\*John J. Studzinski

### TREASURER

\*George Lund

### DIRECTORS

Stéphane Abrial

Todd Achilles

\*Peter Ackerman

Timothy D. Adams

\*Michael Andersson

David D. Aufhauser

Barbara Barrett

Colleen Bell

Stephen Biegun

\*Rafic A. Bizri

\*Linden P. Blue

Adam Boehler

Philip M. Breedlove

Myron Brilliant

\*Esther Brimmer

R. Nicholas Burns

\*Richard R. Burt

Michael Caivey

Teresa Carlson

James E. Cartwright

John E. Chapoton

Ahmed Charai

Melanie Chen

Michael Chertoff

\*George Chopivsky

Wesley K. Clark

Beth Connaughty

\*Helma Croft

Ralph D. Crosby, Jr.

\*Ankit N. Desai

Dario Deste

\*Paula J. Dobriansky

Joseph F. Dunford, Jr.

Thomas J. Egan, Jr.

Stuart E. Eizenstat

Thomas R. Eldridge

Mark T. Esper

\*Alan H. Fleischmann

Jendayi E. Frazer

Courtney Geduldig

Meg Gentle

Thomas H. Glocer

John B. Goodman

\*Sherri W. Goodman

Murathan Günel

Amir A. Handjani

Frank Haun

Michael V. Hayden

Amos Hochstein

Tim Holt

\*Karl V. Hopkins

Andrew Hove

Mary L. Howell

Ian Ilnatowycz

Wolfgang F. Ischinger

Deborah Lee James

Joia M. Johnson

\*Maria Pica Karp

Andre Kelleners

Henry A. Kissinger

\*C. Jeffrey Knittel

Franklin D. Kramer

Laura Lane

Jan M. Lodal

Douglas Lute

Jane Holl Lute

William J. Lynn

Mark Machie

Mian M. Mansha

Marco Margheri

Michael Margolis

Chris Marlin

William Marron

Gerardo Mato

Timothy McBride

Erin McGrain

John M. McHugh

Eric D.K. Melby

\*Judith A. Miller

Dariusz Mioduski

\*Michael J. Morell

\*Richard Morningstar

Georgette Mosbacher

Dambisa F. Moyo

Virginia A. Mulberger

Mary Claire Murphy

Edward J. Newberry

Thomas R. Nides

Franco Nuschese

Joseph S. Nye

Ahmet M. Ören

Sally A. Panter

Ana I. Palacio

\*Kostas Pantazopoulos

Alan Pellegrini

David H. Petraeus

W. DeVier Pierson

Lisa Polins

Daniel B. Poneman

\*Dina H. Powell

McCormick

Robert Rangel

Thomas J. Ridge

Gary Rieschel

Lawrence Di Rita

Michael J. Rogers

Charles O. Rossotti

Harry Sachinis

C. Michael Scaparrotti

Ivan A. Schlager

Rajiv Shah

Kris Singh

Walter Slocombe

Christopher Smith

Clifford M. Sobel

James G. Stavridis

Michael S. Steele

Richard J.A. Steele

Mary Streett

\*Frances M. Townsend

Clyde C. Tuggle

Melanne Verveer

Charles F. Wald

Michael F. Walsh

Gine Wang-Reese

Ronald Weiser

Olin Wehington

Maciej Witucki

Neal S. Wolin

\*Jenny Wood

Guang Yang

Mary C. Yates

Dov S. Zakheim

### HONORARY

### DIRECTORS

James A. Baker, III

Ashton B. Carter

Robert M. Gates

James N. Mattis

Michael G. Mullen

Leon E. Panetta

William J. Perry

Colin L. Powell

Condoleezza Rice

Horst Teltschik

John W. Warner

William H. Webster

*\*Executive Committee Members*

*List as of May 21, 2021*





# Atlantic Council

The Atlantic Council is a nonpartisan organization that promotes constructive US leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today's global challenges.

© 2021 The Atlantic Council of the United States. All rights reserved. No part of this publication may be reproduced or transmitted in any form or by any means without permission in writing from the Atlantic Council, except in the case of brief quotations in news articles, critical articles, or reviews. Please direct inquiries to:

Atlantic Council  
1030 15th Street, NW, 12th Floor,  
Washington, DC 20005  
(202) 778-4952  
[www.AtlanticCouncil.org](http://www.AtlanticCouncil.org)

HOUSE ARMED SERVICES COMMITTEE  
SUBCOMMITTEE ON INTELLIGENCE & SPECIAL OPERATIONS  
*Hearing on Countering Weapons of Mass Destruction*

May 4, 2021

SPEAKERS

Ruben Gallego (D-AZ) *Chairman*  
Rick Larsen (D-WA)  
Jim Cooper (D-TN)  
William Keating (D-MA)  
Filemon Vela (D-TX)  
Mikie Sherrill (D-NJ)  
Jimmy Panetta (D-CA)  
Stephanie Murphy (D-FL)

Trent Kelly (R-MS) *Ranking Member*  
Austin Scott (R-GA)  
Sam Graves (R-MO)  
Don Bacon (R-NE)  
Liz Cheney (R-WY)  
Michael Waltz (R-FL)  
Scott Franklin (R-FL)

WITNESSES:

- Jennifer Walsh (Principal DASD Homeland Defense and Global Security)
- Dr. Brandi C. Vann (Acting ASD-NCB)
- VADM Timothy G. Szymanski (Deputy Commander, U.S. Special Operations Command)
- Rhys M. Williams (Acting Director, Defense Threat Reduction Agency)

GALLEGO: Good morning. Today we will be hearing testimony regarding the current and projected state of the defense apparatus to counter weapons of mass distraction. The witnesses represent the Department of Defense's extensive infrastructure necessary to comprehensively plan for, track, and mitigate the growing threats which compromise weapons of mass destruction.

Even with recent demonstrations by authoritarian regimes to deploy biological and chemical weapons against their own citizens, the threat of WMD is often understood as a high yield nuclear nation killers; however, emerging biotechnologies and illicit narcotics could be weaponized and present existential threats to the country.

Synthetic biological weapons increase the opportunity for a less sophisticated adversary to create chemical and biological weapons without requiring funding, infrastructure, or materially historic--anything that is material historically necessary.

Further, the 2021 Annual Threat Assessment provided by the Director of National Intelligence highlights the growing threat from the development of chemical precursors to produce illicit narcotics such as fentanyl which has already devastated segments of the U.S. population.

The COVID-19 pandemic has shown just how devastating biological threats can be. In this case, the novel coronavirus was not weaponized, but it could be. I am interested in hearing what we are doing to firmly detect and deter these amorphous threats. These threats are exacerbated by the rapid proliferation of accessible technologies, which are often easily accessible for commercially available, creating an omnipresent threat that must be considered strategically while preparing to confront the threats tactically.

With that, let me introduce our four witnesses who are responsible for the modernization of the department's WMD Strategy, policies, and programs to reflect today's threat environment with capability and needs of tomorrow.

We look forward to hearing their testimonies regarding this cold topic, the Honorable Jennifer Walsh, Principal Deputy Assistant Secretary of Defense for Homeland Defense and Global Security; the Honorable Brandi C. Vann, acting Assistant Secretary of Defense for Nuclear, Chemical, and Biologic Defense Programs and Vice Admiral Timothy Szymanski, Deputy Commander of U.S. Special Operations Command and Dr. Rhys M. Williams, Acting Director Defense Threat Reduction Agency.

Ladies and gentlemen, thank you. I look forward to your discussion and will now recognize Ranking Member Kelly for his opening remarks.

KELLY: Thank you, Mr. Chairman, for your opening remarks and your leadership in organizing this morning's posture hearing. Today we will hear from four experts across (INAUDIBLE) North Korea and various terrorist organizations that I look forward to hearing about during this session.

The continued use of chemical weapons by the Assad regime, the poisoning of Alexei Navalny and Sergei Skripal of Russia, and research of biological weapons by China are just a few highlights of this threat. A growing concern brought to the forefront from the ongoing coronavirus pandemic is the threat of biological weapons directed at our military and private citizens. The risk of weaponized aerosol fentanyl is just one example of many alarming and growing threats.

I am interested to hear from our witnesses today on what we are doing to not only identify these types of threats, but also what we are doing to mitigate the threats both for our deployed troops and our citizens here in the homeland. I am also interested to hear our witnesses' views on the global threat posture, especially in the context of great power competition and potential for kinetic engagement with adversaries like China.

Lastly, I am deeply concerned about how the Biden administration's budget will affect our overall counter-weapons of mass destruction preparedness. The ongoing use of chemical threats, coupled with the effects seen from the coronavirus, illuminated the direness of this, and it seems like failing to properly invest in these resources will have grave consequences. I wanted to thank our witnesses in advance for their time today.

I look forward to the continuing work with our counter-WMD experts during the 117th Congress to ensure we are appropriately postured to meet and defeat the threats shaped by weapons of mass destruction. Mr. Chairman, I yield back.

GALLEGO: Thank you, Ranking Member Kelly. I greatly appreciate your comments and dealing with me. Next, thank--now we are going to move on to questions and hearing from our witnesses. We will start with Mrs. Walsh. You are now recognized.

WALSH: Thank you. Chairman Gallego, Ranking Member Kelly, and members of the subcommittee, I am honored to testify on the Department of Defense's efforts related to Countering Weapons of Mass Destruction or CWMD.

DOD's CWMD mission is to dissuade, deter, and, when necessary, defeat actors of concern who threaten or use WMD against the United States and our interests. I work alongside the members of this panel to develop the policies, strategies, capabilities, and expertise needed to accomplish this mission. My written statement describes the WMD threat landscape, and I want to emphasize that the department continues to improve its ability to dissuade, deter, and defeat these threats while maintaining the ability to respond to and mitigate the effects of WMD use.

We are taking action to meet WMD challenges, and as the nature of WMD threats is evolving, we know we have more work to do. The department has three lines of effort to organize our work to counter WMD threats, prevent acquisition, contain, and reduce threats and respond to crises.

To prevent acquisition or contain existing threats, the department leverages its unique tools and expertise in support of a whole of government approach to mitigate the risk of global WMD proliferation and threat actors' pursuit of WMD advancements.

Examples include supporting global norms under the Nuclear Nonproliferation Treaty or NPT, remaining postured to conduct WMD interdiction and preparing partners to do so, and implementing United Nations sanctions to prevent North Korean illicit trade.

Second, the department leads the Cooperative Threat Reduction or CTR program, which works with partner nations to secure and eliminate WMD and WMD-related materials. The DOD CTR program is active in more than 30 countries and has helped a number of these to more rapidly identify and respond to COVID-19.

CTR is called the Nunn-Lugar Program after the two visionary senators who championed its creation, and I want to thank Congress for its continued support for CTR, which has made and continues to make valuable contributions to U.S. and global security.

Third, we developed the capability and capacity of the joint force, allies, and partners to operate in a chemical, biological, radiological, or nuclear, or CBRN contaminated environment. As the department increases focus on competition among great powers developing the capabilities necessary for us to fight and win in a CBRN contested environment in those theaters becomes critical.

The department also works with our allies and partners to confirm that U.S. CBRN defense capabilities are interoperable and to encourage partner nations to share the burden of defense. Achieving effects across this mission space is a departmentwide effort, and we must make hard choices about how we prioritize our activities and investments.

The DOD CWMD Unity of Effort Council brings together 20-plus stakeholders across the department to collaborate on CWMD policy and strategic goals. In 2020 the council helped create inaugural departmentwide CWMD priorities approved by the secretary of Defense. In 2021 we are conducting an implementation review to assess departmentwide alignment with these priorities and guidance.

As administration officials direct and develop new national and departmental strategy reviews and guidance documents, DOD's CWMD stakeholders will be focused on addressing the dynamic CWMD threat and ensuring that it gets space in these documents, including posturing the department to mitigate biological threats more effectively and improving readiness for CBRN challenges in Europe and Asia.

Chairman Gallego, Ranking Member Kelly, and members of the subcommittee thank you for the opportunity to testify today and thank you for your continued support of the CWMD mission. I look forward to our discussion.

GALLEGO: Thank you, Ms. Walsh. Now let's move to Dr. Vann.

VANN: Good morning, Chairman Gallego, Ranking Member Kelly, and the distinguished members of the subcommittee. It is an honor and a privilege to testify before you today on behalf of the men and women of the Department of Defense who comprise the United States Counter Weapons of Mass Destruction enterprise.

These dedicated Americans work tirelessly to defend our brave servicemembers, the nation, and our international partners and allies from the increasing threat posed by the most devastating weapons created.

I would also like to thank my fellow witnesses for their dedication and commitment to our joint enterprise through which we are able to defend the nation and our warfighters from WMD. The CWMD enterprise ensures the United States maintains its enduring technological advantage when countering present and emerging threats.

The NCB office, including the Defense Threat Reduction Agency, is responsible for ensuring the department maintains the capability and readiness to counter WMD across the threat landscape. To that end, the NCB office is aligning ourselves to meet the direction given by the president's interim national security strategic guidance and the secretary's three priorities.

Our efforts will enable us to close today's gaps, rapidly mitigate vulnerabilities, anticipate emerging threats, and strengthen our domestic and international partnerships, but the pace of technology continues to move faster and faster, and as a result, the players on the world stage are shifting, the conflicts landscape is changing and so are the hazards that we all face making our jobs ever more complex.

Overcoming these changes and the emergence and re-emergence of a unique CBRN threats requires the department first to understand that emerging threats landscape and then develop adaptive capabilities to respond to these threats as they arise.

In doing so, we can ensure that the joint force can fight and win in CBRN contested environments, prepare for surprise from emerging threats and reduce the risk that they pose. To modernize the force, the department will work closely with Congress as we shift emphasis from legacy systems to cutting-edge capabilities.

We are moving to get ahead of the threat by anticipating and understanding the convergence of novel science and technological advances, and as a part of layered defense, we can deny the effects of WMD by developing and fielding a wider range of defensive equipment.

Further, fields such as artificial intelligence, machine learning, additive manufacturing, and rapid medical countermeasure development all provide us an opportunity to adapt our defense capabilities quickly and effectively.

We should embrace the technological revolution within the private sector and lead game-changing technology advancements to ensure our warfighters are best prepared for the future threat. Finally, the NCB enterprise will expand our collaborations with our interagency and international partners as well as the private sector to spur innovation, deepen interoperability, and leverage best practices.

Our strong relationships with our allies has brought us incredible value to our ability to protect, detect and mitigate our forces against WMD threats and have informed great strides in our ability to develop and acquire technologies from our force. The NCB enterprise remains focused on anticipating the future threat by closing capability gaps and ensuring the joint force prevails in a contaminated environment. We will continue to remain behind the warfighter and ahead of the threat to ensure our joint forces' ability to survive, operate, and regenerate combat power in the future.

On behalf of the NCB enterprise, I would like to thank the committee for its support and dedication to improving our capabilities to address the current and emerging threat space. Chairman Gallego, Ranking Member Kelly, thank you again for the opportunity to testify, and I look forward to answering your questions.

GALLEGO: Thank you, Dr. Vann. Next, we will have Vice Admiral Szymanski.

SZYMANSKI: Good morning, Chairman Gallego, Ranking Member Kelly, and members of the subcommittee. Thank you for the opportunity to represent the United States Special Operations Command today. On behalf of General Clarke, it is my privilege to join Ms. Walsh, Dr. Vann, and Dr. Williams at this hearing on how we will work together to address some of the most critical national security challenges facing our country.

In 2017 unified command plan directed U.S. SOCOM to coordinate the CWMD mission across the department, and General Clarke have sustained that strategic course. The 2021 unified command plan reiterates U.S. SOCOM's responsibility for planning the department's CWMD efforts as directed by the secretary.

We conduct strategic planning, assess the department's execution of the CWMD campaign, make recommendations to the chairman of the Joint Chiefs of Staff and secretary of Defense, and sustain a DOD-wide functional campaign plan that enables the joint force to improve coordination in countering transregional WMD threats.

The landscape of nuclear, chemical, and biological threats has continued to evolve over this past year. We monitor and analyze progression of existing and over-the-horizon WMD programs closely with essential support from the Defense Intelligence Agency.

The classification level of this forum limits the detail I can provide from our vantage point, but news headlines are a good indicator of the complexity and the nature of the threat.

We have seen norms against the use of chemical weapons continue to erode following Russia's attempted assassination of a former Russian intelligence officer with a Novichok nerve agent in the United Kingdom in 2018 and more recently, the attempted assassination of Russian opposition leader Alexei Navalny with another Novichok nerve agent in August 2020.

China meanwhile is continuing the most rapid expansion and platform diversification of its nuclear arsenal in its history, and it intends, as the director of National Intelligence made clear, and this year's annual threat assessment to at least double the size of its nuclear stockpile during the next decade and to field a nuclear triad. And finally COVID-19 pandemic is a stark reminder of our collective vulnerability to biological threats.

Clearly, WMD are complex transregional challenges that demand the application of specialized expertise and authorities across our government as well as our foreign allies and partners. The Department of Defense plays a unique and critical supporting role to our interagency colleagues, especially at the Departments of Energy, State, Treasury, and Commerce, as well as our law enforcement entities to prevent and contain WMD threats even as we prepare to respond to WMD crises.

We coordinate, therefore, across not only the Department of Defense but also with interagency colleagues and foreign allies and partners without whom achieving U.S. objectives would be exceedingly difficult. We also work closely with the joint staff, combatant commands, and services to regularly assess the department's

CWMD campaign and ensure the department's plans appropriately address changes in the WMD threat environment.

We strive to improve our methodology and ensure it provides timely, reliable, relevant, and actionable information to support senior department decision-making. Our aim is to better support senior leaders charged with employing our joint force today, developing and preparing for tomorrow, and helping to design a military that is ready to fight and win against both current and future WMD threats.

In closing, General Clarke and I would like to thank the members of this subcommittee for their support of this important national security mission. It is a privilege to work together with our colleagues to keep our country safe from the threat of nuclear, chemical, and biological threats. We look forward to our continued partnership with them, with members of Congress, and with our interagency and international partners to ensure our safety now and into the future. Thank you.

GALLEGO: Thank you, Admiral, and now we have Dr. Williams.

WILLIAMS: Chairman Gallego, Ranking Member Kelly, and distinguished members of the subcommittee thank you for your continued support of the Defense Threat Reduction Agency or DTRA. On behalf of the nearly 2200 members at DTRA I am proud to appear today alongside my federal witnesses to talk about our unique role enabling the Department of Defense, the U.S. interagency, and our many international partners to counter and deter weapons of mass destruction and emerging threats.

The Department of Defense established DTRA to integrate and focus the department's expertise against the real and ever-evolving threat of the proliferation and use of weapons of mass destruction or WMD. Under national and departmental policy and guidance and through close collaboration across the department, interagency, and our international partners and allies DTRA delivers innovative capabilities that ensure a strong, protected, and prepared joint force.

Part of DTRA's unique value stems from our dual roles as a defense agency and a combat support agency. In our defense agency role, we respond to requirements from the services as well as from the DOD offices, including the undersecretaries of Defense for Acquisition and Sustainment, Policy and Research, and Engineering. These lines of authority give us strategic roles in the counter WMD fight through nuclear mission assurance, trading verification, building partnership capacity, and cooperative threat reduction, among many key programs.

In our combat support agency role, DTRA's response to the combatant commands and joint staff requirements offering subject matter expertise, operational analysis, and material and nonmaterial solution sets in support of counter-WMD planning and operations.

These roles on behalf of both national security policy and the warfighter enable us to integrate efforts such that at home and abroad, we deliver mission success to detect, deter, and defeat WMD and emerging threats.

I cannot overstate that people are DTRA's most valuable resource. Our staff includes world-class scientists developing therapeutics for emerging pathogens and chemical threats, technical linguists that help find common ground in complex international engagements, tactical specialists securing dangerous weapons and materials, and subject matter experts on call 24/7 to provide real-time expertise and decision support analysis to all levels of government.

DTRA's military personnel ensure that we maintain a close alignment with warfighter requirements, and our capabilities are further amplified by our forward presence at the combatant commands, within task forces, and at key inter-agency locales. In addition to its unparalleled workforce, DTRA is an agency characterized by partnerships and collaboration.

The Center of Excellence for Global Counter-WMD expertise, DTRA works closely with technical peers in academia and in industry. We team with interagency partners like the Departments of State, Energy, Homeland Security, and Health and Human Services and engage equally well with international partners.

This network spanning the breadth of the counter-WMD and emerging threats enterprise allows DTRA to use its unique expertise to wide-ranging effect providing integrated solutions from across the spectrum of competition and conflict.

There are few greater challenges to U.S. national security than those posed by WMD in emerging threats. As the globalized threat landscape revolves DTRA's uniquely skilled workforce and robust collaborative network of partners are ready to evolve with it continuing to safeguard the lives and interest of the U.S. and our allies abroad. Thank you for your time and invitation to participate today, and I look forward to your questions.

GALLEGO: Thank you, Dr. Williams, and thank you for hosting us a couple of weeks back. We are going to now move on to the question period. Each member will have five minutes to ask questions. We will alternate between minority and majority, and I will take the first question.

We can only defeat the threats from weapons of mass destruction with collective action in concert with our allies, partners as well as international bodies. I am concerned that we are not working as closely as we should with countries such as South Korea, India, and Japan.

How close are we working with South Korea to succeed in the CWMD mission? Is there anything preventing you from sharing collaborating with our friends in South Korea? And then lastly, how prepared--well, let's just go that and let's just start with those two questions and can we start with Dr. Vann and then Ms. Walsh you could answer my first two questions and if you need me to repeat them please just ask.

VANN: Yes, thank you, Chairman Gallego, for that question. I think that it is important to say that when we are developing technologies for our joint force, we do work with our allies and partners significantly--excuse me, in order to assess and test equipment and integrate our forces.

Specific to the Republic of Korea, we have active in-country engagements with our allies in Korea that is seeking to not only partner in their readiness but also in reviews of our capabilities with our Korean counterparts. The rest of it, I guess I will defer to Ms. Walsh for a response.

GALLEGO: Thank you, doctor. Ms. Walsh?

WALSH: Thank you very much. With any of our bilateral defense relationships, the issues that we raise, and the capability or capacity development that we work together, it is a bilateral process, and so it's not just about the U.S. offering. It's about another country being a willing partner.

With respect to the Republic of Korea, we have very close bilateral relationships mil to mil across the chemical, biological and nuclear cooperation. The cooperative threat reduction program has activities across the chem-bio and nuclear space. We are working with our Republic of Korea allies to ensure that we are ready for a WMD



contingency regardless of what the threat is. The Koreans bear responsibility; we bear responsibility to ensure that what we have committed to each other is on track and that we can deliver those capabilities.

We meet annually in a CWMD bilateral forum with our Republic of Korea counterparts so that we can ensure that we have trust and confidence, and then obviously, U.S. Forces Korea has daily contact with their Korean counterparts. These issues are definitely top of the list of concerns threats, and therefore these get attention to be sure that we are prepared to work with them.

You had also asked about Japan. With Japan, discussions about WMD are handled through our bilateral relationship channels. The Cooperative Threat Reduction program is not active in Japan, but I can assure you that we speak regularly about ensuring that through extended deterrence and U.S. capabilities that these conversations do happen on a bilateral basis with our Japanese counterparts.

With respect to India, we through--in addressing biological threats, the Cooperative Threat Reduction program facilitates a track to biosecurity dialogue, and then through the Cooperative Threat Reduction program with respect to nuclear issues we have--we support a track 1.5 dialogue with our Indian counterparts. Dr. Williams is probably in a better position to speak to the details since he has oversight of CTR implementation.

WILLIAMS: Thank you, ma'am. That is one of the things--

GALLEGO: (INAUDIBLE) please.

WILLIAMS: The only thing I would add, sir, is that in as far as the Republic of Korea goes to amplify what both Dr. Vann and Ms. Walsh said, we have very close contact with our colleagues both on the R&D side of the house as well as in the Cooperative Threat Reduction space so much so that we recently last year just prior to COVID hosted the Chairman of the Joint Chiefs (INAUDIBLE) from the Republic of Korea at DTRA for a full day of discussions and cooperative agreements in that we routinely have teams going back and forth and we also have an embedded team as was said at U.S. Forces Korea that has constant communication with our allies there in Korea.

GALLEGO: Thank you, Dr. Williams. And Dr. Vann, how prepared are U.S. forces in Korea for a CWMD situation, and how prepared are South Korean troops? I was talking to you yesterday like my WMD experience was on the way to the Syrian border, basically getting handed atropine and being told to just put this in my leg in case something goes bad, which is not good.

(LAUGHTER)

VANN: Yes, sir. Not optimal for sure. So our forces that are currently in Korea first let me say what we do to focus our programs is we actually have a service board that sits with us as we develop RDA, research development and acquisition, capabilities for the joint force structure. We use that service more to help identify capability requirements for the joint force as well as help integrate into and across the larger force modernization efforts.

So in terms of our capabilities for the joint force for chemical and biological defense, we have rapidly developing capabilities that we are delivering every single day. Last year we developed over a million pieces of protective and detection equipment for our forces. We have layered defense approaches as well, so that goes from everything from a detection both remote and point as well as diagnostic gear, physiological monitoring,

personal protective equipment as well as mitigation capabilities for disinfection or decontamination of any of our equipment and personnel.

In addition to that, we are continuing to invest in medical countermeasures for CBR threats to get ahead of the atropine and to make both vaccination or pretreatments as well as post-exposure therapeutics more easily adaptable to new and emerging threats as well as more effective in its pursuit to mitigate the effects of chemical and biological weapons.

GALLEGO: Thank you, Dr. Vann, and Admiral, earlier we were talking about working with their allies. Is there something in our classification process right now that doesn't make it optimal for us to be able to share information with our allies or even across the service in order for us to basically be ready for the CWMD threats of the future?

SZYMANSKI: Chairman, thanks for the question. I think over the years that SOCOM has had the coordinating authority, we have really tried to break down the barriers to sharing information. I know just in the conferences that we coordinate through the year, we always have whatever NDS, WMD threat challenge that we are examining that year we try to have the partners, as we have a day, it's usually a two or three-day conference and we usually have a day where our foreign partners are asked to join and participate in the conference.

Now there always are security classification challenges that we continue to try to overcome. I think a good example is really what we have been doing to help NATO both in their biological and chemical preparedness and response as well as their allied tactical publication that allows for more information sharing. But information sharing outside of WMD has always been one of those obstacles to collaboration that really needs to be examined in the moment for the problem you are trying to solve at hand.

GALLEGO: Thank you. I yield to Ranking Member Kelly.

KELLY: Thank you, Mr. Chairman. Thank you to you witnesses for being here.

GALLEGO: Ranking Member Kelly, I think I went way more than five minutes, so please take whatever time you may need.

KELLY: (INAUDIBLE)

GALLEGO: Ranking Member Kelly one second. Is it just my connection? You are breaking up.

KELLY: Can you hear me?

UNKNOWN: It is hard to hear Ranking Member Kelly here in the HASC hearing room.

KELLY: All right, how about now?

GALLEGO: Yeah, that is better.

KELLY: All right. As the department balances this shift in resources between (INAUDIBLE), with GPC, what are the most significant capability or resourcing vulnerability to counter weapons of mass destruction mission and I will start with you, Vice Admiral, and then the others can chime in?

SZYMANSKI: So the resourcing challenges I think in General Clarke's statement a few weeks back, he talked about the balance between readiness and modernization and as we shift to strategic competition. The CWMD problem set, the way we look at the CWMD problem set it is robust, and it's complex, and it's transregional, and there is really as we think about balance of those resources across all of the threat vectors from the most, the VEO with the most rudimentary applications or developments of CWMD problem to the strategic competitors who have advanced capabilities across the biological, chemical and nuclear you know threat spectrum.

So from a SOCOM perspective and from I think through a department's perspective, we look at the CWMD challenge that it doesn't really shift across--we have to still look at that challenge across all of those threat vectors, so the shift did not really--hasn't really changed the way we attack or go after and try and fight the challenge of the CWMD problem set. Over.

KELLY: Anyone else want to add?

WALSH: I would like to join in and add that one of the reasons that the Unity of Effort Council undertook a DOD-wide CWMD prioritization effort was because we recognize this spectrum of threats is crowded and that resources are always going to be more limited than the threats will bear and so by prioritizing the greatest WMD threats and associating those with where the Department of Defense has the exclusive mission to counter so a leading versus a supporting other U.S. government departments and agencies it's going to help all of our CWMD stakeholder components focus their investments, activities, and efforts toward those priorities.

It does not mean that we are taking our eye off the entirety of the threat spectrum, but it is helping us make smart investments, and one of the things that we continue to look at is where we can invest or multiple returns on the same investments whether it's nuclear, chemical or biological threats that we are countering. Thank you.

KELLY: Thank you, and I spoke with three of the four of you yesterday, and one of my biggest concerns is that as we shift to global power competition that this is a zero-sum game when we talk about this arena, and it is important that we not only focus on global power, but we also look at violent homegrown terrorist nations which can do us much, much damage.

Second, this is for you, Dr. Williams. We have been tracking the SARS-CoV-2 origins and DOD DTRA funding to the Wuhan Institute of Virology through its grantee EcoHealth Alliance. I would be interested if and how (INAUDIBLE) partner of choice for the government agency given its ties to the PLA.

WILLIAMS: Sir, I'm afraid you cut out for the middle of that question. Sir, if you could repeat it, please. Over.

KELLY: I'm talking about the Wuhan Institute of Virology and tracking the SARS-CoV-2, and I am wondering what kind of risk assessment or risk analysis we conducted and how the Wuhan Institute of Virology became the partner of choice for U.S. government agency given its ties to the PLA.

WILLIAMS: Sir, thank you for your question. So as we have looked at this extensively as you know, sir, there was a request from the Congress to the department a year or two years ago to look at this funding level as well as again most recently. We have done a thorough look at all of our programmatic activities to ensure that the Defense Threat Reduction Agency's funding to this NGO was not provided to the best of our knowledge into the Wuhan Institute of Virology.

On top of it, sir, our expertise both on programmatic as well as kind of our technical expertise looks at all of our activities that we invest in for these types of NGOs to make sure that the risk for government funding is minimalized and in keeping with the traditions and the boundaries of the federal acquisition process but equally as importantly policy as well. I think Dr. Vann, did you want to add anything to this?

VANN: I don't have much to add to that. I think that is a good, you know, good review, but I would like to add that we also across the NCB did a thorough review to identify any potential access or investment into the Wuhan laboratory, and we have not identified any. It is something that we continue to watch to ensure that our investments are not going to places where they should not be.

KELLY: Mr. Chairman, I want to ask a last question, but I'm going to ask that they submit for the record where we don't take all of the time on the hearing. I just want to ask how confident each of you are (INAUDIBLE) chemical and biological capabilities of our adversaries and if there are gaps, please in writing let us know what we can do to close some of those gaps, and with that, Mr. Chairman, I yield back.

GALLEGO: Thank you much. I now yield time to Representative Larsen.

LARSEN: Thank you, Mr. Chair. I hope your dog stays off of you this time. So my question is really about legacy, and I might have difficulty asking this because I have legacy thinking myself, so I have to switch my brain a little bit in trying to craft this question.

I think it's for Vice Admiral Szymanski and Director Williams and given what we know and what you have testified to regarding synthetic biology, regarding 3-D printing, advanced manufacturing, these different technologies that both have uses good and evil who is in charge at the department for ensuring that the women and men in our military understand that their uses of these technologies generally and then understanding the uses of these technologies in the field?

I can think of a mini 3-D printing advanced manufacturing plant being deployed with a group of women and men in our military in the field for use for certain purposes. Who is in charge of educating and upscaling these women and men for the uses of these technologies?

SZYMANSKI: So thank you for the question, Congressman Larsen. Really there's a service requirement and responsibility largely for the force generation (INAUDIBLE) manned, equipped, and trained.

From a coordinating authority from SOCOM, our responsibility is really about the planning, helping the combatant--geographic combatant commands plan against how to counter WMD, and annually we look and assess against that plan the changing conditions on the ground, the changing threat vectors, the changing situation and assess if that campaign plan and that framework is as adequate and needs to be adaptable.

I think that the collaboration between what SOCOM does as the coordinating authority and then what DTRA does I think more importantly to your question is that DTRA really gets after the unique solutions of those gaps that we identify and that plan against those changing conditions.

For instance, we may see a new biological threat. Do we have the diagnostics, and I think Dr. Vann was pretty articulate in her opening statements about the kinds of things that they are doing across the spectrum of being prepared as well as to maintain consequence as well as protective equipment capabilities.

But largely the man training (PH) and equipping aspects for our individuals for men and women are a first responsibility. The geographic combatant commanders' responsibility for how we incorporate the plan as it relates to the threat in their region.

LARSEN: So do we have to rely on the services then to generate that requirement if we see it otherwise? If we see that they aren't doing that?

SZYMANSKI: No, sir. Often we will help generate that requirement for them. In fact, this year, this is the first year that SOCOM has done a comprehensive from a coordinating authority lens has submitted a broad-based requirements piece for DOD to and each of the geographic combatant commanders to DTRA.

LARSEN: All right. Dr. Williams?

WILLIAMS: Sir, so as the admirals said, sir, yes, we ingest that requirements from the services as well as from the geographic combatant commanders on a routine basis. We actually get four-star requirements that come in, and we rack and stack those against the available resources and again keeping with policy to make sure it's there.

As the admiral just said, I literally sent last night to General Clarke in a response on that requirements letter that came in earlier this spring. So what we end up doing is also as part of our engagement with the services under man, equip and train aspect of things we make sure we bring that cutting-edge technology knowledge back into their training courses as it exists. A specific example of that, sir, we actually run the Defense Nuclear Weapons School, which trains all of the nuclear aspects of that.

LARSEN: Dr. Williams, anything more please for the record, and I will have questions for Dr. Vann and Ms. Walsh regarding your definition of legacy as well more on the prioritization efforts of the (INAUDIBLE) interested in the outcomes of that. So with that, I will develop (PH) for the record Mr. Chair, and I will yield back. I will yield back none of the time I have and the time left.

GALLEGO: Thank you, Representative Larsen. Now we have Representative Scott next.

SCOTT: Thank you, Mr. Chairman, and ladies and gentlemen, thank you for being with us today. The topic kind of really better discussed, I think behind closed doors, but I want to encourage my colleagues to get up to speed if you are not on the ABMS system and some of the potential gaps or - not potential - but the very real gaps that we have in the ability to pick up weapons that could and would be used against the United States if we were to find ourselves in a conflict with Russia or China.

The systems are smaller, they are significantly faster, and that means we have got to pick them up with systems that we use in space, and I will mention a couple of my concerns with that is that a few years ago, we were dependent on rockets from Russia to actually launch satellites at the United States and I am happy to use the private sector to help us launch satellites, but I do think that we need to be self-reliant and not dependent on the public sector to do that and so that is one thing that I hope the agency, the Defense Department will continue to look at is making sure that while publicly traded companies are fine to use during times when we are not in conflict what would happen to our ability to launch if we were dependent on publicly-traded companies during an all-out war with Russia and China.

As we talk about ABMS versus the legacy systems and Admiral, this is predominantly for you because you have been one of the guys on the ground as a special operator. I am very concerned about the communications aspect of the new systems, and as we move to space, are you confident that we can handle the communications from space and not necessarily from aircraft for our special operators?

SZYMANSKI: Congressman, thank you. Thank you for the question. Space and communications, as we think about strategic competition, I think it's a problem set that we think about often. You are right as special operations has historically been dependent on robust tactical communications and a lot of that is based on space architecture; I would also say you are right that this would be a better discussion in another setting at another time but let me say this.

I think it's important that we run scenarios. In fact, we have just run a scenario down at SOCOM not related to CWMD on a day without coms, and so how do we plan for everything from a tactical to our strategic coms to take and survive a hit so and good military planning as you know we do most likely courses of action scenarios and we do most dangerous and so what do we need to--what are the gaps in things like cloud computing, communications at the edge and so we're kind of going through that analysis now and how resilient and how resilient does that kind of infrastructure have to be?

Obviously, our space communications are important, and I think we are taking a hard look at how we will be able to fight and win in a contested or denied com environment.

SCOTT: Space is going to be contested as well, and I understand the concept and I won't get too much into it. I actually like the concept, but I do want to make sure that, you know, if we did end up in a scenario where we needed to be doing a lot of launches that we would not be totally dependent on publicly-traded companies to do that, and we got ourselves in a bind a couple of years ago where we were depending on Russian rockets to actually launch our satellites, and I hope that is something that we just pay attention to. It's a mistake we made in the past; we don't need to make it in the future.

I will mention one last thing for my colleagues on the Democratic side. In the President's speech, he mentioned the DARPA-like program in the National Institute of Health. I'm not so sure that it wouldn't be better served to the general public if we did a National Institute of Health type program under DARPA so that we did effectively the same thing the President is asking for, but the model and the leadership of DARPA seems to work very well, and I don't see why we can't increase that funding over there with a specific focus on health. With that, my time is up, as you just heard, and so I appreciate all of you, and I look forward to continuing the discussion.

GALLEGO: Thank you, Representative Scott, and impressive that you keep your own timer. Now let's move on to Representative Keating.

KEATING: Thank you, Mr. Chairman. I thank our witnesses. Public reports, including a very recent one with the National Academy of Sciences, have detailed the threats behind some directed radio frequency energy weapons and how that can be used. Are you doing any research or involvement in that in terms of (INAUDIBLE)?

WALSH: I had trouble hearing the question--understanding the question.

KEATING: I will try again. Public reports, including the National Academies of Sciences, have talked about directed radio frequency, microwave (INAUDIBLE) kind of weapons, energy weapons that were used. Are you (INAUDIBLE) what kind of (INAUDIBLE)?

GALLEGO: Were you able to understand that question?

WALSH: I believe so, thank you. The Department of Defense is aware and supporting a whole of government effort looking into those issues. This is another topic that would be happy to discuss in a different setting.

KEATING: There are; however national publications done, for instance, the National Academy of Sciences, so can you just comment generally on whether they present a real danger?

WALSH: What the National Academy of Sciences report assessed is definitely something that we are continuing to look at. It was directed at the request, I believe, of the Department of State, and so we are taking that report and its findings seriously. It is part of what we are looking into with cooperation with the State Department and other parts of the U.S. government.

KEATING: All right. I realize that we probably will have to deal with more of this in a classified setting but thank you very much. I yield back, Mr. Chairman.

GALLEGO: Thank you, Representative Keating, and I now actually lost check of who is next. Give me one second, please. Representative Bacon, you are up.

BACON: Thank you, Mr. Chair. Thank you to all of our panelists. I appreciate your leadership. My first question is to Ms. Vann. Is Iran your number one threat for nuclear proliferation? Thank you.

VANN: Actually, I think for that conversation, I would defer to my colleague from policy.

WALSH: Thank you very much. When it comes to proliferation, we have great concerns about China. China has lax export controls, it is not a country that exercises in great transparency in reporting to international bodies it has signed up to report to but also just in being good stewards of public information sharing. So we do have concerns about China, the proliferation that could support WMD activities across the board of items coming out of China, and China not responsibly monitoring what is going where.

Obviously, we look at any number of proliferation concerns when it comes to nuclear. This could include fissile material, radiological material. Iran is not on my--it is not my number one proliferation threat. Iran does not have a nuclear weapons program so, but there are other nuclear weapons--

BACON: What I think you answered it (INAUDIBLE) recipient of that proliferation, so that was the intent of my question. Framed that way, is that a concern Iran working with China?

WALSH: I would want to take that conversation into a classified conversation, sir.

BACON: Unclassified documents that China (INAUDIBLE) so I am concerned about what were some potentially seeing with Iran as well. Just this week, DIA said that Al Qaeda is being safeguarded in Iran in an unclassified report from DIA. Are we concerned about Iran colluding with Al Qaeda in other forms of WMD?

WALSH: Sir, we have great concerns about any number of WMD threat actors from state-based through nonstate actors and violent extremist organizations. We rely on the intelligence community DIA leading

member of that to help inform our policy considerations of where are the threats, who has the intent, and where these are colliding, so while I can't speak specifically to the DIA report you were referencing, I can say that we are mindful of and watching where there are these alignments of VEOs and state actors of concern.

BACON: (INAUDIBLE) from Iran, that's a concern. And I want to go with that. Maybe a follow-up question for Dr. Williams. It's a little off-topic, but what is the status of the Open Skies Treaty? The administration has given mixed signals on this. The OC-315 (PH) aircraft are being taken to the boneyard, and yet the administration is saying that Open Skies may not be gone.

WILLIAMS: Sir, thank you for that question. I would really defer that one to Ms. Walsh from a policy perspective on the future of Open Skies.

WALSH: Thank you. I think this is one that is under review right now, and so I am not in a position to speak to that, but I would be happy to consult with my colleagues who have the lead for the Open Skies Treaty and circle back with you and your team, sir.

BACON: Thank you. I will just (INAUDIBLE). It seems to be making a statement there, but then to say you have maybe not abandoned Open Skies it's mixed signals. I surely would like to know where we are going with that, so thank you very much, and I yield back.

MURPHY: Thank you, Mr. Bacon and Chair Gallego had to step away for a moment, so I will be standing in for him, and it just so happens I am next on the list, so I will yield to myself to ask some questions here.

I just want to thank the witnesses. You know the ODN Annual Threat Assessment has said that China, and you all said it in your opening that they are undertaking one of the most rapid expansions in platform diversification of its nuclear arsenal in history and has pretty much indicated they are not interested in any arms control agreements. Also Mrs. Walsh, Ms. Walsh, you just mentioned that it's been difficult to work with them due to lack of transparency and other such things.

While I recognize the conversation about their nuclear arsenal might be better suited for a classified setting, what I do want to ask about is an area where they exhibit some of the exact same behavior of lack of transparency, lack of cooperation, and that is in the area of their fentanyl production, and I just hosted a panel featuring witnesses from the DEA and ONDCP regarding China's role in America's opioid crisis.

They have been sending precursor chemicals to countries like Mexico, where they are made into fentanyl at labs and then mixed with other illicit drugs before they make their way to our homeland, where they kill Americans, and they are destroying communities all across this country.

So and I think the threat assessment also highlights that Mexico will certainly make progress this year producing high-quality fentanyl using these very chemical precursors from China. So the question is to Ms. Walsh and Dr. Vann how is the department modernizing its capabilities to attract the production and shipment of such chemical precursors from Asia to the Western Hemisphere?

WALSH: There are any number--thank you very much, congresswoman. There are any number of communities across DOD that are looking at this issue just from different perspectives. Our counter narcotics and global threats organization, even the DOD CWMD Unity of Effort Council took up the issue of Fentanyl I believe it was two years ago now.



And so across many threads we are looking at what are the precursors, where are they coming from? We have bilateral conversations, multi-lateral conversations to make sure that countries that are the source and origin of these are aware of what's going on underneath their nose. Giving them the opportunity and trying to persuade them to take action to regulate, curtail, be more aware if not cease entirely what it's doing.

Part of the challenge is that there are very legitimate uses of Fentanyl. So this is the--this is the space between the legitimate and then the illicit use with that. And I'll defer to Dr. Vann who's more of an expert on this.

VANN: Yes, thank you, ma'am. The--Fentanyl is a -- as Ms. Walsh said is a interesting space because it highlights some of the dual use nature of and dual use dilemma that we now face where we have a legitimate use as well as a potential for nefarious use.

In terms of capability development that we have against things like the Fentanyl classes we have a very robust RDA activity to ensure that our joint forces have the right detection equipment to identify--both detect and identify any potential Fentanyl in the environment as well as a diagnostic capability so that you can see when there is a potential human exposure to classes of Fentanyl as well as personal protection equipment as well as our ability to treat any potential exposure.

So focusing specifically on delivering manned portable medical countermeasures that could be utilized by the force if exposed to those agents.

MURPHY: Thank you. And this is to the admiral. You know, it strikes me that when we talk about CWMD or countering violent extremists there--or countering transnational organizations that deal in sort of the illegal substances, there are a lot of similarities. Sometimes there's state actors nefariously involved. There are networks of people who are moving illegal money, drugs, and other illegal substances. Are there lessons that we--can be learned from our decades of working counterterrorism that can be applied in CWMD or countering narcotics?

SZYMANSKI: Congresswoman, thanks for that questions. Yes, there are absolutely lessons learned from the, you know, countering violent extremist organizations and the things we've done to build networks, to defeat a network. And I think what you've really just described is the basis of our functional campaign plan which is about the pathway to defeat. And it's a pathway whether it's a -- I'm sorry, did you have a question?

MURPHY: No, we're just out of time. And just to be mindful of everybody else's time. I'm sorry to interrupt you, I'd love to get your response through a question for the record. And that's a conversation I'd like to continue at a different time. And with that I will yield to the next speaker. Mr. Franklin.

FRANKLIN: Yes, thank you, Representative Murphy. I'm on the road and I apologize. But I do have some questions. I'm just submitting those to the record. But didn't want to drive and try to ask questions at the same time.

MURPHY: Great. Well travel safely and we'll look forward to your questions for the record. Next, I have Mr. Larsen.

LARSEN: Think--are we going back to a second round then, Chair?

MURPHY: I think it appears that we must be.

LARSEN: I just don't feel--okay. Alright. Great. So I'll circle back to some ideas for my questions for the record. But for Ms.--Ms. Walsh, can you speak more particularly to the prioritization efforts in the Unity of Effort Council? What can you share with us about which legacies you're looking at, which are going to survive, which aren't, and honestly what new technologies that we need to put more time into which re--would require us to not put time into other systems.

WALSH: Our department priorities started with an intelligence assessment of looking at what are the WMD threats to U.S. interests and the U.S. homeland in particular? Where are those threats coming from? Looking at threat actors: who has the capability, who is trying to get more or different capability, who is modernizing whatever capabilities they already have? On top of the intelligence analysis we looked at policy considerations as well.

We blended these to assess what are the threats? More than a specific technology, it's about the threat actor. Because it's the actor who will use any given technology or capability and that's what we have to counter. So while I'm not able in this environment to walk you through what those priorities are, we would certainly be happy to have a follow up conversation with you and share those priorities.

There -- and they differentiate because it could be that one actor has a -- is further along in one type of W--posing one type of WMD threat than another. And so we do look at these by WMD threat and actor, bring them together, and that's how we've come up with our priority list.

LARSEN: Can you answer the question in this environment about relative DOD or other agency investment? Is it gonna require us to move money around to not spend as much on X to do--to do Y? Or Z?

WALSH: Our priority process did not tease out that level of decision. What I will expect is that as we go through an implementation review this year of looking at how are our components applying these priorities into their particular areas of responsibility I think that's where we will start to determine if we have more, fewer, or different investments to make. But this is also where we're going to look at can we get multiple returns on similar or same investments.

LARSEN: Yeah. Yeah. So I have a definition of legacy investments in the DOD after 20 years in Congress. A legacy investment is something that the DOD doesn't want to do that Congress won't let them get rid of. So just a heads up to, you know, maybe bring us along as you work on this set of priorities so that we aren't surprised as the oversight folks. That'd just be my one rule of caution on this. I'm open to the smart people of the DOD looking at this obviously.

It's just sometimes you run into a buzzsaw called Congress because sometimes we don't wanna get rid of something or sometimes we're surprised by the result. So I think it's just important that if--especially if it comes down to making not just a priority choice but also then it gets to where does the money go to invest in that priority, I think -- just a word of advice on that. And with that, Chair Murphy, yeah, I'll yield back. Thank you.

MURPHY: Thank you, Mr. Larsen. And next I yield to Ranking Member Kelly.

KELLY: Thank you, Chairwoman Murphy. And just given the increased use of chemical weapons in Syria and that have (INAUDIBLE) in Russia, what can we do to curb further use of chemical or biological weapons? What are we doing to ensure international norms against the use of these weapons is not eroded or to develop new standards to deal with the emerging chem and bio threats?

WALSH: I don't think I heard all of your question--please circle back. You did break up a little bit in there. But what I think I heard you say is you're interested in knowing what we are doing to help preserve international norms, prevent further erosion of them on the chemical and biological side. I will say it starts with--it starts with our own behavior and being a leader through international fora and through your bilateral relationships.

In--in response to Russia's 2018 use of a Novichok, the United States along with likeminded countries worked it--through the OPCW to add the Novichoks to these Chemical Weapons Convention schedule or the list of prohibited items that country--signatories agree that--that will not be used. We have continued to speak out when we have seen international norms either eroded or flagrantly violated.

We do not want any nation to be able to think that they are going to get away with this. And so diplomacy is our first course of action. The Department of Defense stands in support of the Department of State. We work hard to maintain bilateral relationships so that other countries are speaking out when they are outraged by Russia and other nations' behavior as well. We continue to encourage bilateral and multilateral public dialogues about biological agents through biological surveillance, detection, investments that we are making in partner countries.

We are helping to build others' capacity to not only be able to detect but also then to diagnose and contain biological outbreaks that are naturally occurring. We are asking and calling on our partners and likeminded allies to speak out on these issues. COVID has certainly put a premium on that in the last year that we need to take this seriously. This is not a niche issue and this is one that can have devastating consequences to security, economic, and just a general public health as well.

KELLY: Very quickly I asked a question earlier and I still would like a more in depth--cause I think a lot of this is gonna be classified. But I would like to follow up. It's just how confident are we that we have the full appreciation of the chemical and biological capabilities of our adversaries?

WALSH: At an unclassified level I can tell you that we do have concerns because of Russia and China's lack of transparency in meeting its obligations to notify through the Chemical Weapons Convention and the Biological Weapons Convention. That lack of transparency, behavior we've observed over the last year, of intentional misinformation about U.S. capabilities, U.S. investments, and partner nation biological laboratories that are serving public health and public good.

But Russia and China continue to put out propaganda that--that's giving false information about what the--what those facilities are and what our partner nations are doing. So I do not have trust and confidence that we know everything. They are not living up to their end of the bargain.

KELLY: Very good. And just very quickly. I'm signing off after this. I wanna thank you witnesses again for your testimony here today and for what you do every day to keep this nation safe. With that I'm signing off (INAUDIBLE). I'm sorry (INAUDIBLE) but I'm sure one of my Republican (INAUDIBLE)--

GALLEGO: Thank you, Representative Kelly. And then I will--assuming Representative Scott will act as ranking member after you leave. Okay. Excellent. Next, we have on my list--thank you for bearing with me. I actually jumped off to attend another hearing. Representative Keating I have next on my list.

KEATING: For second round, Mr. Chairman, I'll yield back.

GALLEGO: Excellent. Then after that we have Representative Scott.

SCOTT: I don't have any further questions, Mr. Chairman. I just again would love to have the subcommittee come to Robins Air Force Base, look at the ABMS system and, you know, just making sure that we're again, our dependency on foreign sources for rocket fuel and our dependency on the private sector I just wanna make sure that we work through those issues and that while we can always count on the private sector in times of peace, you know, what would we do in a time of war with regarding our ability to launch.

With that I'll yield. Well, after thank the members of the panel for their service.

GALLEGO: Thank you, Representative Scott. I have Representative Murphy next if you have a second round.

MURPHY: Thank you, Mr. Chair. Actually, I would just like to let Admiral finish the answer to the previous question I had regarding the lessons off of CT and whether or not we're applying them in this area of counter narcotics as well as counter WMD.

SZYMANSKI: Congress--Congresswoman Murphy we ab--we absolutely are applying those lessons. I think you--you're aware that SOCOM is also the coordinating authority for violent extremist organizations. And we've been obviously in that--in that fight for almost two decades. And as I was starting to say earlier, you know, all this is really about the pathway to defeat. And so when we look--we--at whether it's transnational criminal organizations, counter violent extremist organizations, other bad actors, all are dependent on certain pathways.

And we call those the transregional enablers. So it's things like comms, finances, and those things. So understand a network regardless of what the--what the illicit aspects of what is being transferred it -- there are absolutely lessons learned from what we've done over the years and that--with, you know, great participation of our partners as well as the intelligence community on being able to understand networks really then try to understand their activities on how they use those trans-regional enablers and how we get after those enablers to actually prevent and or counter whatever the illicit cargo is or whatever the high value leaders that we need to get after.

MURPHY: So as a member who represents Florida, I'm always very concerned with what's going on in Latin America and the Caribbean and that's an area where there's quite a bit of transnational criminal organization activity. Are you aware of any traditional WMD threats to the United States from state or non-state actors emanating from Latin America or the Caribbean?

SZYMANSKI: Ma'am, I--thank you for the question. I would prefer to take that question for the record and do it in a--in a more classified setting.

MURPHY: Great. Thank you. And then final question for you, Admiral. There--with the U.S. preparing to withdrawal its troops from Afghanistan in September of this year there are a lot of national security risks that are involved with this decision as we all know. And I know you're working through a lot of those to mitigate and prepare for them.

Can you discuss how you think withdrawal might affect America's counter WMD efforts in Afghanistan and the neighboring countries? Especially if the Taliban gains strength and if Afghanistan once again becomes a haven for terrorist groups that have an interest in using WMD. How can we and our allies combat these threat without a significant permanent force presence on the ground?

SZYMANSKI: Congresswoman I--again I--I'd like to take that--that one for the record. But I--I think it--there will be a significant partner and ally piece. There's a lot doing into right now from the State Department with di-diplomacy. With a number of the neighboring countries in the Gulf coalition countries. There is a recent--a couple recent intelligence assessments on--after withdrawal. And I would prefer to talk about those in a classified setting on--where--there's a lot of hope for also where the Taliban will be in--for wanting to be recognized as an international order.

So we understand the--it's a very uncertain time. And at the moment we're really focused on the safe and deliberate retrograde of all the troops and all the other U.S. and foreign personnel that are currently deployed in Afghanistan.

MURPHY: Great. I understand the need to move this conversation to a different classification level and look forward to the opportunity to do that. Thank you to the witnesses today and I yield back my time. Thank you, Mr. Chair.

GALLEGO: Thank you, Representative Murph--Vice Chair Murphy. Now I'd like to move to Representative Waltz.

WALTZ: Yeah, thank you, Mr. Chairman. And I--I'd just like to associate myself with Representative Murphy's remarks and questions, particularly in the wake of the withdrawal. I think one of the things that's being lost in the conversation is that even if all of our--all of our best hopes bear out and the Taliban has had a change of heart and decides to be a responsible international actor, no one has been able to explain to me to date including General Miller what capability they have to enforce any agreement against Al-Qaeda and half the world's terrorist organizations on, you know, what capability did they have that 300,000 Afghan Army Soldiers and 40 Western nations have struggled to do over the last 40 years.

But along those lines I would certainly welcome if we have a follow on classified brief I'd certainly love to participate in that. My question is operationally when it comes to IEDs, Dr. Williams, DTRA I think has done a great job of over the years of training our Afghan partners, our partners in the Afghan Army in counter IED detection and defeat.

My understanding is those trainers and those assets are being withdrawn. What leave behind capability through the Afghan Security Forces Fund, whether it's IED detection kits, nitrate kits, what leave behind capability are we providing to the Afghan Security Forces through your programs?

And I understand there's a State Department--I co-signed a letter for the State Department through its program to also provide funding so that we don't have to go back. Which I sadly fear that we're going to have to do. But to bolster the Afghan Security Forces' ability to deal with IEDs which by the statistics I'm seeing account for 75 percent of their casualties.

WILLIAMS: Sir, thank you for your question. One point of clarification as you know, sir, the former counter IED activities that were done through the Defense Threat Reduction Agency are actually transitioning at the end of this fiscal year into the Army. For continuing use for that. In terms of your answer--or your question about leave behinds, sir, as the admiral said I think I would like to prefer and take that in a--in a classified setting so we can have a little more fulsome discussion on that, sir.

WALTZ: Okay. I'll just say I hope that we're not taking that for the record because there's not really a plan yet. I know that I'm sure you're working on it. And I struggle to understand why it's classified if we're handing it over to the Afghans. But that's fine. We'll take that to a different setting.

The other piece that I'd like to talk to that I would imagine would be this setting is I know there's a number of classified programs dealing with Pakistan's nuclear program and assuring the security of those assets. So that I would like to request in a classified setting. And the status of those programs with no presence in Afghanistan. And then finally again, probably also classified, so Mr. Chairman, my questions will be pretty brief. But I'm incredibly concerned and have asked this question in the past.

If we move to any type of conflict on the Korean Peninsula I understand there's a number of programs with SOCOM, DTRA, and others to secure North Korea's nuclear assets. My concern is what type of deconfliction if any that we've had with China who would obviously also want to assure that those assets are secured. So that would be I guess then three requests for you in a classified setting.

And Mr. Chair, if I could just--one more before I close. I'm still not clear when we have that why a leave behind capability with the Afghans so that they can detect IEDs, I'm not sure why that would be classified. I mean that should be I think--

GALLEGO: --Would not be possible. I'm sorry. Repeat yourself--

WALTZ: --And so that--so that we can assure everyone that they have that capability. But I'll just take that for the record and I yield. Thank you, Chairman.

GALLEGO: Thank you, Representative Waltz. And I think--I believe it is my turn now. Yes it is. Okay, great. The Department of Defense recently in 2017 transferred the Countering Weapons of Mass Destruction mission lead from U.S. Strategic Command to U.S. Special Operations Command, signaling a shift in strategy that places greater emphasis on identifying and preventing threats before they metastasized into a crisis.

In addition, the Department of Homeland Security used to have a CWMD Office, consolidating numerous offices and functions across the Department. How does coordination work at the national level to ensure the CWMD activity authority, policy, planning, and expertise are operating cohesively and effectively and efficiently, and what progress has SOCOM made to develop the inf--infrastructure, partnerships, expertise, strategy, and tactics needed to address this mission successfully?

Let's start with vice--with the admiral.

SZYMANSKI: Chairman thank you for the question. So for the years that SOCOM has had the func--or, excuse me, the coordinating authority for CWMD it's really the basis of the whole effort is built on the functional campaign plan (PH). And building the comp--helping the Combatant Commanders with their campaign plans (PH)--(INAUDIBLE) Combatant Commanders.

As I kind of mentioned it in one of the opening questions with the threat vectors or the threat actors in--in their regions to how we put that plan together in coordination with the geographic Combatant Commander, how we assess that plan against the changes to the threat, against the changes to the actors, as well as the environment and then make recommendations on any material gaps, training deficiencies, et cetera.

But what we do in the meantime back here in D.C. or in CONUS is we hold a couple seminars a year called the--our coordination sem--coordination seminars. Our senior leader seminars.

We bring together a number of folks from partners and allies to interagency to many members largely from the Unity of Effort Council across joint staff in DOD and look at a very specific problem. And then we try to bring in a whole of government approach to how we might answer that, identifying not only the gaps in the Departments--in the Department of Defense's capabilities but also potentially think more use of what Department of Energy, Department of State, Department of Commerce could apply to that problem set.

But that from a SOCOM Coordinating Authority, that's really planning and assessing and recommending. I think I would go--defer to Ms. Walsh on the Unity of Effort Council and how they use the existing processes to pull the other things that you talked about in the beginning of your question.

WALSH: Thank you very much, admiral.

GALLEGO: Thank you, Ms. Walsh.

WALSH: The Unity of Effort Council was created after we recognized that we had a lot of cooks in the kitchen, but we weren't working off of the same recipe. And so through the Unity of Effort Council we have convened 20 different stakeholder organizations across the Office of the Secretary of Defense, various joint staff components, all of the services, SOCOM is our coordinating authority.

And then all of our Combatant Commands, so that we can raise awareness among these components of what their roles and missions are, what issues that have been stuck or are emerging, and where we need to work together to make sure that these issues can rise to the surface so that senior leaders are aware of threats, opportunities, capabilities we have but also areas where we need to develop further capabilities or make different investments.

And over the course of the last several years I would argue that we have built not just awareness, but we have built connective tissue that didn't exist previously. And so now we have in a phrase of--the consolidated buying power of the CWMD community and DOD is yielding benefits.

Our plans, our strategy documents, our resource requirements, our understanding of threats, our understanding of where we can have cross pollination, but also our understanding that some components don't necessarily sit in all of the meetings where resource decisions are made or requirements are decided or prioritized. And then where the strategy documents are.

So through the Unity of Effort Council, we have taken both a bottom up but also a top down approach in identifying what are those issues that do not get resolved in other existing DOD fora? And through this we have given rise to a community that is now speaking--that is understanding more but is also speaking with more of one voice. We expect that we will continue to see dividends from the Unity of Effort Council as the Department goes through the strategic review and guidance development efforts this year.

Whether it's the global posture review, the next National Defense Strategy, and then any number of other reviews that the Department is conducting, I am confident that our Unity of Effort Council members will be able to bring WMD issues more into the forefront. Thank you.

GALLEGO: Thank you, and--Ms. Walsh. And just a general statement. I, you know, I feel like the--across the federal government there is really good unity and conversations happening about countering WMD measures. I worry when it needs to come across down to your local police and state government. And one of the things I think we saw from 9/11 was that, you know the--as much as the federal government's important it's also your local government that's important in terms of prevention and deterrence and what--even unfortunately maybe sometimes reactions.

So I just wanna kind of remind that we keep that in mind going to the future. I have on my list for a second question if he wants it, Representative Waltz. Do--is there anybody else that has another question they don't wanna--Representative Scott, do you have any, ranking member, that anybody from your side--okay, great. Excellent.

Well thank you so much for your time to all of our presenters. You know, I did know that there was a lot of things that were said that were gonna have to go for the record or in a classified setting. Please make sure to follow up with our staff to actually, you know, fulfill that. I think there's a lot of things that we want to follow up and there's no need for us to leave things hanging up in the air.

Thank you for your time and I hope to see you all soon.





# CONGRESSIONAL UPDATE

December 15, 2021



## HEADLINES

- **Senate:** The upper chamber will be in session this week, and possibly next, as they attempt to complete three priority items before the holidays: the debt limit, the NDAA, and the Build Back Better Act – a \$2 trillion climate and social spending bill. The debt limit was approved yesterday and today the NDAA was agreed to and sent to the President. SASC also sent the JCS Vice-Chair nomination of ADM Christopher Grady to the floor.
- **House:** Yesterday, the House completed their work for the week with votes on the debit limit, combating Islamophobia, barring the importation of goods made with forced Uyghur labor, and holding Mark Meadows in contempt of Congress over his refusal to comply with the January 6th special committee. This is likely the final week in session for the House this year.
- **NDAA:** The Senate voted to pass the \$768 billion defense bill today by a vote of 89-10. The measure now goes to the President for his signature. The bill language is identical to the text that was released last week. A key provision on EcoHealth Alliance bars any funding of projects conducted in China. Funding-wise, notable increases include \$105 million more for BTRP and \$5,877 million more for overall RDT&E.
- **Debt Limit:** Yesterday, both chambers approved of the final step to raise the debt limit by another \$2.5 trillion. The bill's passage sets up another showdown on the debt ceiling as soon as November 2022.
- **Nominations:** DoD nominees (b)(6) CIO) and (b)(6) (Operational Test & Evaluation) were confirmed yesterday. However, with 158 nominees blocked over holds placed by conservatives on other key posts, Senate Majority Leader Schumer has threatened to keep his chamber in session over the weekend and into next week to get movement on the slate. Two Republican Senators have placed holds on high profile Defense and State Department nominees over their objections to related administration policies. Sens. Ted Cruz and Josh Hawley have pledged to maintain their holds until they get a vote on sanctions over the Nord Stream 2 pipeline effort and more accountability over the pullout of troops from Afghanistan, respectively.

## KEY HEARING SUMMARY

### Biosecurity for the Future: Strengthening Deterrence and Detection

- 8 Dec, 1000
- House Foreign Affairs -- Subcommittee on Asia, the Pacific, Central Asia & Nonproliferation
- Witnesses:
  - (b)(6) (Nuclear Threat Initiative)
  - (b)(6) (Johns Hopkins University-School of Public Health)
  - (b)(6) Council on Strategic Risks; Former ASD-NCB)
  - (b)(6) (Sculpting Evolution Group, Massachusetts Institute of Technology)
- **Summary:** Discussion alternated between the prevention and defeat of naturally occurring health challenges as well as acts of bioterrorism. The chairman advocated for improved international

biosecurity systems, but also praised advancements and investments in efforts such as gene sequencing, bio surveillance, and detection. The ranking member was critical of China's efforts to hide COVID, highlighted the fact that lab accidents are frequent, and sought a better enforcement mechanism for the Biological Weapons Convention. Former ASD(NCB) (b)(6)

(b)(6) focused on a "deterrence through denial" strategy for biological weapons that would render any bio threat ultimately unsuccessful through the availability of sufficient countermeasures. He stated that we have the technologies today to make this strategy a reality.

(b)(6) optimism was contrasted by the testimony from (b)(6) who was highly critical of scientists who seek to learn and share which viruses could cause new pandemics as their research will eventually assist bioterrorists. (b)(6) called out Eco Health Alliance as a prime culprit in this area and blasted federal funding for making it all possible. (b)(6)

(b)(6) encouraged the panel to support more focused research as opposed to the "overly broad surveillance and basic analysis" that is currently conducted to combat zoonotic events. He also expressed support for vaccines and felt that the medical community should be more proactive in pushing back on anti-vaccine elements. Finally, (b)(6) promoted a three-pronged approach to biosecurity, which included (1) stronger global norms, (2) development of a reliable system for attribution and accountability, and (3) an increased financial commitment from the U.S. and global partners to make these goals a reality.

## NOMINATIONS

### Department of Defense:

- *Confirmed (Date)*
  - (b)(6) DoD Chief Information Officer (14 Dec)
  - (b)(6) – Dir, DoD Operational Test & Evaluation (14 Oct)
- *Intention to Nominate (Date Announced)*
  - (b)(6) er Secretary of the Navy (13 Dec)
  - (b)(6) SAF Asst. Secretary-Financial Management & Comptroller (13 Dec)
  - (b)(6) Army Asst. Secretary-Manpower & Reserve Affairs (8 Dec)
  - (b)(6) USD-A&S (Nov 30)
- *Reported to Full Senate (Date reported)*
  - (b)(6) – Vice Chair, Joint Chiefs of Staff (14 Dec)
  - (b)(6) – DUSD Personnel & Readiness (8 Dec)
  - (b)(6) – Army General Counsel (8 Dec)
  - (b)(6) – DUSD for Policy (28 Oct)
  - (b)(6) – ASA Acquisition, Technology & Logistics (28 Oct)
  - (b)(6) – USN General Counsel (28 Oct)
  - (b)(6) – Under Secretary of the Army (21 Oct)
  - (b)(6) – DUSD for Research & Engineering (21 Oct)
  - (b)(6) – USAF Asst. Secretary-Acquisition, Technology, Logistics (21 Oct)
  - (b)(6) – Asst. Army Secretary for Installations & Environment (21 Oct)
  - (b)(6) – USAF Asst. Sec.-Manpower & Reserve Affairs (21 Oct)
- *Nomination Hearing Held (Date of Hearing)*

- (b)(6) – ASD Manpower & Reserve Affairs (7 Oct)
- *Nominated (Date SASC received)*
  - (b)(6) – USAF Asst. Secretary-Installations, Energy & Environment (6 Dec)
  - (b)(6) – DoD Inspector General (15 Nov)
  - (b)(6) – ASD Sustainment (15 Nov)
  - (b)(6) – USAF General Counsel (21 Oct)
  - (b)(6) – ASD-Homeland Defense & Global Security (10 Aug)
  - (b)(6) – ASD-Space Policy (4 Aug)
  - (b)(6) – ASD International Security Affairs (23 Jun)

**Other National Security Posts:**

- (b)(6) – DHS Under Secretary for Intelligence & Analysis (17 Nov received by SSCI)
- (b)(6) – Special Representative, Bureau of International Security & Nonproliferation (19 Oct reported to full Senate)
- (b)(6) – Assistant Secretary of State for Arms Control, Verification and Compliance (5 Oct hearing held)

**CRS REPORTS OF INTEREST**

- U.S. Strategic Nuclear Forces: Background, Developments & Issues (14 Dec 2021)
- North Korea's Nuclear Weapons and Missile Programs (13 Dec 2021)
- AUKUS Nuclear Cooperation (10 Dec 2021)
- Nuclear Cooperation with Other Countries: A Primer (8 Dec 2021)

**From:**  
**To:**  
**Subject:**  
**Date:**

(b)(6)

DIR Staff Meeting  
Thursday, January 20, 2022 11:06:00 AM

---

Steve,

Do you have anything that I can put out in the Directors MTG.

(b)(5)

(b)(6)

Division Chief, Integration Management Division

Defense Threat Reduction Agency (DTRA)

(b)(6)

Page 195 of 433

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 196 of 433

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 197 of 433

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 198 of 433

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act



Page 199 of 433

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 200 of 433

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 201 of 433

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 202 of 433

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 203 of 433

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 204 of 433

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 205 of 433

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 206 of 433

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act



Page 207 of 433

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 208 of 433

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 209 of 433

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 210 of 433

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 211 of 433

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 212 of 433

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 213 of 433

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 214 of 433

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act



Page 215 of 433

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 216 of 433

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 217 of 433

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 218 of 433

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 219 of 433

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 220 of 433

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 221 of 433

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 222 of 433

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act



Page 223 of 433

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 224 of 433

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 225 of 433

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 226 of 433

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 227 of 433

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 228 of 433

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 229 of 433

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 230 of 433

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act



**From:**  
**To:**

(b)(6)

**Subject:**

DTRA's HASC-ISO Bio Book

**Date:**

Thursday, March 10, 2022 3:35:19 PM

**Attachments:**

HASC-ISO Bio Book CY22 (9MAR22).pdf

---

Team,

Sharing our (b)(6) for HASC-ISO. Hope this is helpful!

V/r,  
Steve

Steve Linton-Smith  
Legislative Liaison  
Defense Threat Reduction Agency  
stephen.a.linton-smith.civ@mail.mil

(b)(6)

**From:**

(b)(6)

**To:**

**Cc:**

**Subject:**

EcoHealth Cong request

**Date:**

Tuesday, May 24, 2022 7:41:21 PM

---

Hi Dawn,

Last year DTRA was asked to produce documents to the Senate Homeland Security Committee. (b)(5)

(b)(6)

Can you determine if those remaining documents have now been reviewed and are ready to release to the committee?

Thanks,

(b)(6)

Legislative Liaison

Defense Threat Reduction Agency

(b)(6)

**From:**

(b)(6)

**To:**

**Cc:**

**Subject:**

EcoHealth HAC-D inquiry

**Date:**

Thursday, June 23, 2022 10:26:48 AM

**Attachments:**

DoD Grants to EcoHealth (1 Apr 22).xlsx

---

(b)(6)

A staffer with HAC-D has inquired about DoD funding of EcoHealth Alliance

(b)(5)

(b)(5)

Thanks!

(b)(6)

Legislative Liaison

Defense Threat Reduction Agency

[stephen.a.linton-smith.civ@mail.mil](mailto:stephen.a.linton-smith.civ@mail.mil)

(b)(6)

**From:** (b)(6)  
**To:** DTRA Ft Belvoir DIR List Task LA  
**Subject:** FW: Follow up RFI from HSGAC - Permanent investigations Subcommittee  
**Date:** Tuesday, May 24, 2022 12:27:14 PM  
**Attachments:** (CATMS1) OSD010438-21 CONGRESSIONAL INCOMING.pdf  
**Importance:** High

---

LA,

Follow up from the prior EcoHealth tasker. (b)(5)

(b)(5)

(b)(6)

V/r,

(b)(6)

Staff Actions Program Manager

Office of the Chief of Staff

(b)(6)

Defense Threat Reduction Agency (DTRA)

Fort Belvoir, VA 22060-6201

-----Original Message-----

From: (b)(6)

Sent: Tuesday, May 24, 2022 11:27 AM

To: (b)(6)

Cc:

Subject: FW: Follow up RFI from HSGAC - Permanent investigations Subcommittee

Importance: High

Chief,

FYSA:

Follow up to the follow up for EcoHealth. (b)(5)

(b)(5)

(b)(6)

-----Original Message-----

From: (b)(6)

Sent: Tuesday, May 24, 2022 10:32 AM

To: (b)(6)  
Cc: DTRA Ft Belvoir Org List DTRA Staff Actions <dtra.belvoir.org.list.dtra-staff-actions@mail.mil>  
Subject: FW: Follow up RFI from HSGAC - Permanent investigations Subcommittee  
Importance: High

EcoHealth never ends.

Looks like a 2nd follow up... (b)(5)

(b)(5)

(b)(6)

-----Original Message-----

From: (b)(6)  
Sent: Tuesday, May 24, 2022 10:24 AM  
To: (b)(6)  
(b)(6)  
Cc: (b)(6)  
Subject: FW: Follow up RFI from HSGAC - Permanent investigations Subcommittee  
Importance: High

(b)(5)

V/r,

(b)(6)

SAIC Contract Support Office of the

Assistant Secretary of Defense for Nuclear, Chemical, and Biological Defense

Programs OASD(NCB) Front Office

(b)(6)

From: (b)(6)  
Sent: Tuesday, May 24, 2022 8:30 AM  
To: (b)(6)  
OU  
Cc:  
Subject: Re: Follow up RFI from HSGAC - Permanent investigations Subcommittee

(b)(6)

The follow up question is:

(b)(5)

V/r

(b)(6)

From: (b)(6)  
<mailto:(b)(6)>  
Date: Tuesday, May 24, 2022 at 8:22:03 AM  
To: (b)(6)  
<mailto:(b)(6)>  
(b)(6)  
Cc: (b)(6)  
<mailto:(b)(6)>  
Subject: RE: Follow up RFI from HSGAC - Permanent investigations Subcommittee

Sirs, I was waiting for CDR Oman to return today. Are you asking us to answer this (I didn't see anything marked #2?)

(b)(5)

V/r,

(b)(6)

SAIC Contract Support Office of the  
Assistant Secretary of Defense for Nuclear, Chemical, and Biological Defense  
Programs OASD(NCB) Front Office

(b)(6)

-----Original Message-----

From: (b)(6)  
<mailto:(b)(6)>  
Sent: Monday, May 23, 2022 2:12 PM  
To: (b)(6)  
<mailto:(b)(6)>  
<mailto:(b)(6)>  
C:  
<mailto:(b)(6)>  
Subject: RE: Follow up RFI from HSGAC - Permanent investigations Subcommittee

(b)(6)

Did you provide a response to this RFI?

v/r

(b)(6)

Legislative & Congressional Oversight (LCO) Office  
Office of the Under Secretary of Defense  
for Acquisition and Sustainment

(b)(6)

-----Original Message-----

From: (b)(6)  
<mailto:(b)(6)>  
Sent: Tuesday, May 3, 2022 4:52 PM  
To: (b)(6)  
<mailto:(b)(6)>  
<mailto:(b)(6)>  
Cc: (b)(6)  
<mailto:(b)(6)>

Subject: FW: Follow up RFI from HSGAC - Permanent investigations Subcommittee

(b)(6)

Please see below follow-on #2 RFI regarding this our response to the HSGAC letter.

v/r

(b)(6)

Legislative & Congressional Oversight (LCO) Office  
Office of the Under Secretary of Defense  
for Acquisition and Sustainment

(b)(6)

-----Original Message-----

From: (b)(6)  
<mailto:(b)(6)>  
Sent: Monday, May 2, 2022 3:49 PM  
To: (b)(6)  
<mailto:(b)(6)>

Subject: RE: Follow up RFI from HSGAC - Permanent investigations Subcommittee

(b)(6)

follow-up question is:

(b)(5)

(b)(5)

V/R,

(b)(6)

Special Assistant  
OASD – Legislative Affairs  
1300 Defense Pentagon  
Room: 3D844

(b)(6)

-----Original Message-----

From: (b)(6)

<mailto:(b)(6)>

Sent: Monday, May 2, 2022 3:44 PM

To: (b)(6)

<mailto:(b)(6)>

Subject: RE: Follow up RFI from HSGAC - Permanent investigations Subcommittee

Thanks (b)(6)

(b)(6)

Legislative & Congressional Oversight (LCO) Office  
Office of the Under Secretary of Defense  
for Acquisition and Sustainment

(b)(6)

-----Original Message-----

From: (b)(6)

<mailto:(b)(6)>

Sent: Monday, May 2, 2022 2:11 PM

To: (b)(6)

<mailto:(b)(6)>

(b)(6)

Cc: (b)(6)

<mailto:(b)(6)>

(b)(6)



(b)(6)

Subject: RE: Follow up RFI from HSGAC - Permanent investigations Subcommittee

(b)(6)

Thanks

(b)(5)

(b)(5)

V/R,

(b)(6)

Special Assistant  
OASD – Legislative Affairs  
1300 Defense Pentagon  
Room: 3D844

(b)(6)

-----Original Message-----

From: (b)(6)

<mailto:(b)(6)>

Sent: Monday, May 2, 2022 12:01 PM

To: (b)(6)

<mailto:(b)(6)>

(b)(6)

Cc: (b)(6)

<mailto:(b)(6)>

(b)(6)

Subject: RE: Follow up RFI from HSGAC - Permanent investigations Subcommittee

(b)(6)

In late 2021, the Senate Committee on Homeland Security and Governmental Affairs, Permanent Subcommittee on Investigations sent a letter to the Secretary of Defense regarding their examination of the public health implications of federal funding provided for virological research (TAB B). Specifically, the subcommittee requested:

- All research proposals or grant applications submitted by or on behalf of EcoHealth Alliance (EcoHealth) and/or the Wuhan Institute of Virology.
- All documents or communications sent by the Defense Threat Reduction Agency(DTRA) in response to any research proposal or grant application submitted by or on behalf of EcoHealth and/or the Wuhan Institute of Virology.

(b)(5)

On March 28, 2022, the subcommittee requested additional information, specifically:

- All unfunded research proposals and grant applications by or on behalf of EcoHealth and/or Wuhan Institute of Virology.
- Clarify DoD's position on the alleged unfunded proposal for WIV, as the co-grantee.

(b)(5)

v/r

(b)(6)

Legislative & Congressional Oversight (LCO) Office  
Office of the Under Secretary of Defense  
for Acquisition and Sustainment

(b)(6)

-----Original Message-----

From: (b)(6)

<mailto:(b)(6)>

Sent: Monday, May 2, 2022 10:59 AM

To: (b)(6)

<mailto:(b)(6)>

(b)(6)

Cc: (b)(6)

<mailto:(b)(6)>

(b)(6)

Subject: RE: Follow up RFI from HSGAC - Permanent investigations Subcommittee

All,

Bumping this up, for everyone's SA.

Today is the response date. HSGAC contacted LA this morning to follow-up. Standing by to transmit when received.

Thanks!

V/R,

(b)(6)

Special Assistant  
OASD – Legislative Affairs  
1300 Defense Pentagon  
Room: 3D844

(b)(6)

-----Original Message-----

From: (b)(6)

<mailto:(b)(6)>

Sent: Wednesday, April 20, 2022 3:57 PM

To: (b)(6)

<mailto:(b)(6)>

(b)(6)

Cc: (b)(6)

<mailto:(b)(6)>

(b)(6)

Subject: RE: Follow up RFI from HSGAC - Permanent investigations Subcommittee

(b)(6)

Yes, 2 May is good.

(b)(6)

FYSA for this RFI, DTRA will respond by 2 May.

v/r

(b)(6)

Legislative & Congressional Oversight (LCO) Office  
Office of the Under Secretary of Defense  
for Acquisition and Sustainment

(b)(6)

-----Original Message-----

From: (b)(6)

<mailto:(b)(6)>

Sent: Wednesday, April 20, 2022 3:31 PM

To: (b)(6)

<mailto:(b)(6)>

Cc: (b)(6)

<mailto:(b)(6)>

(b)(6)

Subject: RE: Follow up RFI from HSGAC - Permanent investigations Subcommittee

(b)(6)

Could DTRA possibly get an extension on this RFI until May 2nd? We have the data ready, but DTRA has a new Director and she requires a bit more time to get spun up on all manner of details.

Please Advise.

Thanks

(b)(6)

Legislative Liaison  
Defense Threat Reduction Agency

(b)(6)

-----Original Message-----

From: (b)(6)

<mailto:(b)(6)>

Sent: Monday, March 28, 2022 10:13 AM

To: (b)(6)

(b)(6)

Cc: (b)(6)

<mailto:(b)(6)>

(b)(6)

Subject: FW: Follow up RFI from HSGAC - Permanent investigations Subcommittee

DTRA,

This came in two weeks ago, I thought it was being worked by our Congressional person, but it was not.

Can you generate an answer to this RFI that I can send along?

V/r

(b)(6)

From: (b)(6)

<mailto:(b)(6)>

Sent: Wednesday, March 16, 2022 2:33 PM

To: (b)(6)

(b)(6)

Cc: (b)(6)  
<mailto:(b)(6)>  
(b)(6)

Subject: FW: Follow up RFI from HSGAC - Permanent investigations Subcommittee

(b)(6)

The attached response was sent to HSGAC and received a follow up RFI:

"The letter asked for all grants applications and proposals, which would include grants that may not have ultimately been funded. It does not appear that the unfunded proposal list is included in the attachment to this production. As I am sure you are aware, at least one such proposal that was allegedly not funded has been made public, and would have included the Wuhan Institute of Virology as a co-grantee. Is it DoD's position that no such grant proposal exists?"

Adding a little detail, the article referred is from Atlantic Article,  
<https://www.theatlantic.com/science/archive/2021/09/lab-leak-pandemic-origins-even-messier/620209/>.  
The project appears to be named DEFUSE.

Please provide a response by 22 March.

Thanks.  
v/r

(b)(6)

Legislative & Congressional Oversight (LCO) Office  
Office of the Under Secretary of Defense  
for Acquisition and Sustainment

(b)(6)

From: (b)(6)  
<mailto:(b)(6)>

Sent: Wednesday, March 16, 2022 2:23 PM

To: (b)(6)  
<mailto:(b)(6)>  
Cc: (b)(6)  
<mailto:(b)(6)>

(b)(6)

Subject: FW: Follow up RFI from HSGAC - Permanent investigations Subcommittee

(b)(6)

This should go to NCB. They wrote the letter that Mr. Hunter signed out.

Respectfully,

(b)(6)

From (b)(6)

(b)(6)

Sent: Friday, March 11, 2022 9:03 AM

To (b)(6)

<mailto:

Cc

(b)(6)

Subject: Follow up RFI from HSGAC - Permanent investigations Subcommittee

(b)(6)

The attached response was sent to HSGAC and received a follow up RFI:

"The letter asked for all grants applications and proposals, which would include grants that may not have ultimately been funded. It does not appear that the unfunded proposal list is included in the attachment to this production. As I am sure you are aware, at least one such proposal that was allegedly not funded has been made public, and would have included the Wuhan Institute of Virology as a co-grantee. Is it DoD's position that no such grant proposal exists?"

Adding a little detail, the article referred is from Atlantic Article, <https://www.theatlantic.com/science/archive/2021/09/lab-leak-pandemic-origins-even-messier/620209/>. The project appears to be named DEFUSE.

Please provide a response by 18 March.

Thanks.

v/r

(b)(6)

Legislative & Congressional Oversight (LCO) Office  
Office of the Under Secretary of Defense  
for Acquisition and Sustainment

(b)(6)

From

(b)(6)

(b)(6)

Sent: Monday, March 7, 2022 6:25 PM

To (b)(6)

<mailto:

Cc

<mailto:

(b)(6)

Subject: Follow up RFI from HSGAC - Permanent investigations Subcommittee

(b)(6)

We sent the attached response to HSGAC and received a follow up RFI:

The letter asked for all grants applications and proposals, which would include grants that may not have ultimately been funded. It does not appear that the unfunded proposal list is included in the attachment to this production. As I am sure you are aware, at least one such proposal that was allegedly not funded has been made public, and would have included the Wuhan Institute of Virology as a co-grantee. Is it DoD's position that no such grant proposal exists?

Not sure who this should go to for a response. I'd appreciate if you could forward as applicable.

V/r,

(b)(6)

I am turning over with my relief, CDR Tim Hurley, USN. Please copy him on all emails you send to me: (b)(6)

(b)(6)

Special Assistant  
OASD - Legislative Affairs  
1300 Defense Pentagon  
Room: 3D844

(b)(6)

**From:**  
**To:**  
**Cc:**

(b)(6)

**Subject:**

FW: The Issue that Never Dies: Ecohealth Alliance

**Date:**

Wednesday, August 17, 2022 11:31:29 AM

**Attachments:**

[image005.png](#)

[image006.png](#)

[image007.png](#)

[image008.png](#)

[OSD010438-21 USS R. Johnson Congressional Response EcoHealth 03012022.pdf](#)

[OSD010438-21 Enclosed.pdf](#)

[OSD010438-21 USS J. Ossoff Congressional Response EcoHealth 03012022.pdf](#)

[2021-11-18 Ossoff and Johnson Letter to DOD re EcoHealth.pdf](#)

(b)(6)

Were you all involved with Senators Johnson and Ossoff's request for details about Ecohealth funding. This request came in in November 2021 and our response was from February of this year. I'm attaching our responses, an enclosure, and the originally letter. The Senators requested all research proposals or grants submitted by Ecohealth alliance and WIV (none for WIV) and all documents or communications sent by the agency in response to any research proposal or grant application submitted by EcoHealth.

(b)(5)

What we really need in the immediate term is to give the Senators an update, which ideally might include an ETA of when this request will be completed.

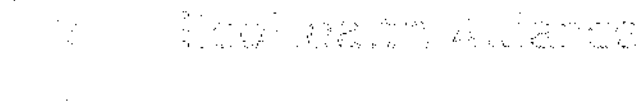
V/r,

(b)(6)

Analyst | Contract Support

Office of the Deputy Assistant Secretary of Defense for Chemical and Biological Defense





# Global Rapid Identification Tool System (GRITS)

## Annual Progress Report (2013-2014)

The GRITS project received base year funding from January 18th, 2013 to January 17th, 2014. On January 17th, 2014, we demonstrated our one-year capabilities to DTRA. The funding period is currently expanded through July 18th, 2014.

## Contents

### A. Summary

### B. GRITS milestones

1. Test RIT encephalitis prototype
2. Test robustness of network models
3. Expand RIT encephalitis prototype
4. Automate data collection
5. Generalize network model
6. Build web app for analysts

### C. Conceptual diagrams

GRITS.md

GRITS.md service

GRITS data services

### D. Screenshots

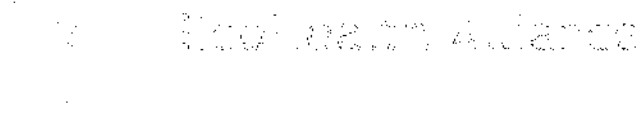
GRITS.app portfolios

GRITS.app portfolio metadata view

GRITS.app annotator

Network visualizations

### E. Visualizations and the Girder database (Kitware)



## A. Summary

This project was initiated as the Rapid Identification Tool (RIT) for undiagnosed diseases. With expanded funding, it evolved into the Global Rapid Identification Tool System (GRITS). This evolution reflects the powerful “system” of tools we developed to extend the diagnostic capabilities to “global” coverage .

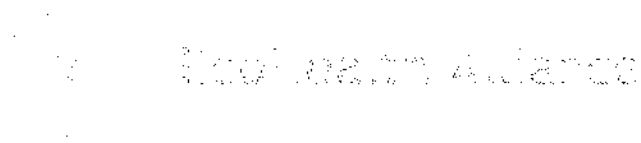
The original prototype was developed by manually extracting symptoms from encephalitis reports in ProMED-mail to train a network model. Through initial testing, we identified modeling approaches that improved performance by combining machine learning and natural language processing approaches with network modeling. We recognized that the diagnostic capabilities could not scale to global coverage or additional diseases without automating data collection and crowdsourcing the data curation. Consequently, we developed the GRITS.app User Interface (UI) to display our tool system alongside our data, including event portfolios, annotation tools, models, and visualizations. We also integrated the project with ongoing EHA initiatives to collect historical disease outbreak data (Global Repository for Infectious Diseases - GRID) and background data for the drivers of disease emergence (EcoHealth Data - EcoHD). Furthermore, we integrated work from our colleagues at Kitware to support the storage and visualization of the large, complex datasets being generated.

With support for an expansion period (through July 2014), we are building a robust and scalable software infrastructure to support advanced media diagnostics. This includes the main web application (GRITS.app), media diagnostics (GRITS.md), and Girder database (GRITS.db). This will provide diagnostic decision support system for analysts that builds upon a network of experts and data from EcoHealth Alliance, HealthMap, and ProMED-mail.

## B. GRITS milestones

The GRITS base project had six (6) major milestones

1. Test RIT encephalitis prototype
2. Test robustness of network models
3. Expand RIT encephalitis prototype
4. Automate data collection
5. Generalize network model
6. Build web app for analysts



Here are the tasks and associated status for the milestones, drawn from the monthly reports.

### 1. Test RIT encephalitis prototype

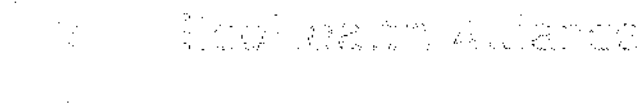
- Held kickoff meeting with subcontractors
- Rewrote encephalitis prototype in the Python programming language (from PERL) to support wide range of natural language and network tools
- Conducted literature review of historic emerging infectious disease events to develop a new global training model for network model
- Updated encephalitis dataset from Gideon
- Applied our new model to undiagnosed disease reports in ProMED-Mail
- New model improves total diagnoses of original ProMED dataset from 76% sensitivity to 81% correctly diagnosed (new data, to be generated in Milestone 3, should further improve diagnostic capability)

### 2. Test robustness of network models

- Reframed original network approach by developing an improved prototype with support vector machines (SVM) as a classifier, which provided better results and more accurate optimization
- Tested alternate approaches to optimizing network structure
- Identified optimal weights that provide a good classifier
- Evaluated alternate validation approach (one-out cross validation)
- Used metric learning as a way of constructing the network and getting weighting between nodes
- Improved disease classification results by replacing pairwise (one against one) approach with individual disease classification
- Explored new classifiers with new metric learning approaches
- Worked with subcontractor Kitware to generate dynamic network visualizations for exploring the Kitware dataset
- Generated probabilities of correct diagnoses from individual disease classification approach

### 3. Expand RIT encephalitis prototype

- Ingested and processed 6 months of ProMED-mail data to begin developing a global testing dataset
- Updated dataset from Gideon for all infectious diseases, and created matrix of

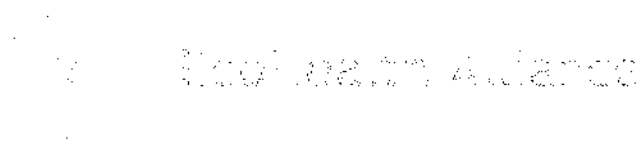


symptoms by disease for model training set

- Configured named entity recognition tool for disease characteristics (e.g. disease, symptoms, location, person, organization, species, genus)
- Expanded model suite (SVM, Naïve Bayes, Decision Tree, Stochastic Gradient Descent, Gradient Boosting, and Extra Trees)
- Prototyped model for identifying novel clusters of disease symptoms
- Prototyped tool for diagnosing unknown disease reports from ProMED
- Prepared live code demo for 6 month evaluation

#### 4. Automate data collection

- Prototyped data harvesting bots for automatically collecting disease data for the network model; we began this task early to expand our datasets
- Added Stanford Named Entity Recognition tool (NER) to the auto-tagging tool set
- Added Symptom and disease matrix from Gideon to the auto-tagging tool set
- Developed capacity to retrain diagnostic model using tags, manually added by users through the web interface
- Developed and ran bot to collect previous 6 months of Healthmap data
- Built network storage graph for Healthmap and Promed data for XData visualizations
- Developed code to auto-tag and diagnose raw text submitted from web interface
- Developed data scraper to collect text from user-submitted URI
- Conducted scientific review to compile a list of historic disease outbreaks
- Collected symptom descriptions from reports on historic disease outbreaks
- Improved auto-tagging tools to handle 349 diseases and 299 symptoms
- Ran auto symptom and disease taggers on 6 months of Promed data
- Analyzed results of auto tagger to develop mechanism for flagging problematic reports to improve accuracy of tagging system
- Identified sources of additional symptom and disease definitions on the web
- Built collection of scripts for data mining symptoms and definitions to train diagnostic tool
- Automatically generated a symptom and disease matrix for H7N9 and MERS
- Automatically generated training data with symptoms only
- Automatically generated training data with presence/absence for mentions of disease characteristics
- Developed capacity to input symptom and disease data mined from the web
- Worked with Kitware to develop data storage mechanisms for GRITS data
- Compared symptoms from gideon and wikipedia to test effectiveness of matrix
- Manually cleaned up scraped symptom definitions



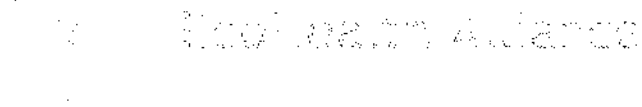
- Compiled list of ontologies
- Aggregated published abstract data from PubMed
- Aggregated Twitter data from SNAP
- Aggregated disease definitions from Google
- Loaded GRITS data resources into CKAN
- Setup preview (maps, graphs, tables) for resources in CKAN
- Developed script to automatically build portfolios from lists of ProMED-mail IDs

## 5. Generalize network model

- Prototyped code for tracking historic symptom evolution to constrain uncertainty around diagnoses for 3 outbreak events
- Setup Jenkins for continuous integration to improve the code base and report failed builds
- Wrote code for tracking historic symptom evolution for 20 outbreak events
- Prototyped matrix-based diagnosis and compared performance with original network model
- Prototyped alternatives to matrices for storing and visualizing the data for the machine learning and network models
- Developed DocPad web application (alternative to Sphinx) for user documentation
- Developed visualizations of error in model input due to evolution of symptom reporting
- Analyzed symptom reporting to understand the evolution of uncertainty for diagnosing nine disease outbreaks
- Developed list of disease definitions
- Developed list of symptom definitions
- Evaluated success of diagnosis tool for reports with varying numbers of diseases mentioned
- Developed Promed report taxonomy from style guide

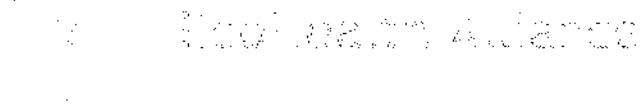
## 6. Build web app for analysts

- Began prototyping a web app for interacting with disease reports; we began this task early to facilitate collaborating on a common model and dataset with our subcontractors throughout the grant
- Prototyped browser-based Javascript network visualizations for ProMED-mail data
- Developed application for the analyst to diagnose disease outbreaks (using Flask



and Backbone.js)

- Built application for analyst to tag word entities in disease reports to expand training dataset
- Deployed tagging application on AWS.
- Allow users to run model generated from manual tags via the tagging UI
- Allow users to run additional data sources as auto-taggers
- Prototyped "Tool Box" - interface to the tools for tagging data and running models
- Produced web visualization for showing results of differential diagnosis (ranked by symptom presence)
- Prototyped "Bot Shop" - interface for monitoring disease alerts
- Prototyped "Data Warehouse" - interface to MIDAS scientific data store
- Prototyped "Disease Sentinel" - interface to multiple global data sets
- Kitware developed visualizations for information, geospatial networks
- Kitware developed text frequency timeline visualization
- Developed web interface to allow users to submit URL or raw text for diagnosis
- Integrated WiggleMaps visualizations of EHA Hotspots datasets in disease sentinel
- Integrated WiggleMaps visualizations of gridded global threats data sets (e.g. conflict, climate, demographics)
- Setup production server on AWS for GRITS web application
- Prototyped "Cabinet" to store collection of disease reports training intelligent diagnosis tools
- Prototyped Slickgrid editor for ontologies and datasets
- Tested d3, datatables, tablesorter, and handson for editing ontologies and datasets
- Developed web application for curating historic disease reports
- Developed web application for administrator to build forms for inputting new disease outbreak data
- Prototyped tool for users to comment and discuss outbreak reports
- Tested CKAN as a data store
- Installed CKAN on AWS
- Prototyped "portfolio manager" as interface to tag reports
- Enabled importing Promed reports into portfolios
- Developed list displays of portfolios and reports
- Highlighted tags in reports and enabled tagging from report
- Brainstormed tag categories and imported to portfolio manager
- Developed inline tagging UI for diseases, symptoms, locations, organizations, host, and transmission
- Developed tag recommendations for most common words, recent words,



popularity, and user contributed

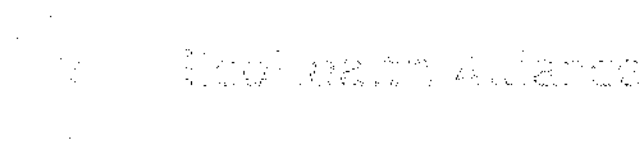
- Built custom display for auto-tagging results and integrating with manual tagging
- Migrated GRITS application to reactive Javascript framework
- Contributed GRITS reactive Javascript code to EHA's Global Repository for Infectious Diseases (GRID)
- Implemented Meteor "Collection API" to expose GRID data to GRITS
- Completed reviews of symptoms from approximately 277 historic disease events (total) in GRID
- Pushed EcoHealth Data (EcoHD) beta instance with CKAN to public IP address (data.ecohealth.io) for referencing from GRITS
- Set up web server to train and run our diagnostic model, and deployed to AWS
- Enabled retraining the model on demand so users can retrain it when new data is added
- Enabled diagnostic model to be trained on either report-level symptom lists or portfolio-level symptom lists
- Manually developed GRITS portfolios for historic disease events and encephalitides
- Separated lists of manually reviewed and candidate tags
- Added automatic highlighting of manually reviewed tags
- Added capability for editor to accept or reject all tags in a category in annotator
- Set up test instance of GRITS on AWS
- Set up test software process with Jenkins on AWS
- Began developing a custom 'reactive-table' for tabular display of reports; testing determined that d3, datatables, tablesorter, and handson were inadequate
- Prepared GRITS, GRID, and EcoHD for demonstration at Digital Infuzion
- Integrated Javascript D3 map visualizations of historic events in GRID
- Set up production instance of GRITS at <http://grits.ecohealth.io>
- Configured software process for production instance of GRITS
- Completed reviews of symptoms from 320 historic events (total) in GRID
- Developed 'reactive-table' to display interactive tabular data and portfolios in GRITS, along with metadata and resource counts
- Pushed 'reactive-table' to Github  
(<https://github.com/ecohealthalliance/reactive-table>) for peer review and contribution
- Created a portfolio view with a list of resources, portfolio metadata (editable), list of tags, and progress bar to show status of manual tagging
- Created script to import additional tags for new disease characteristic categories
- Created script to import portfolios from a spreadsheet, and extract disease, location, and year as metadata



## Information Aquired

- Created Python script to ingest data from Google spreadsheets via API
- Enabled reviewers to manually remove auto-generated tags
- Enabled reviewers to add new tags
- Enabled toggling tags that are highlighted in a resource, and showing or hiding all tags from a category
- Added a manually curated disease-symptom matrix to use in diagnosis for diseases that are not yet in our system
- Integrated diagnosis into portfolio and resource views
- Basic integration of network visualizations from Kitware and DoD XData project
- Created a script to build portfolios from HealthMap queries
- Developed roadmap and sprint schedule for completing expansion SOW tasks



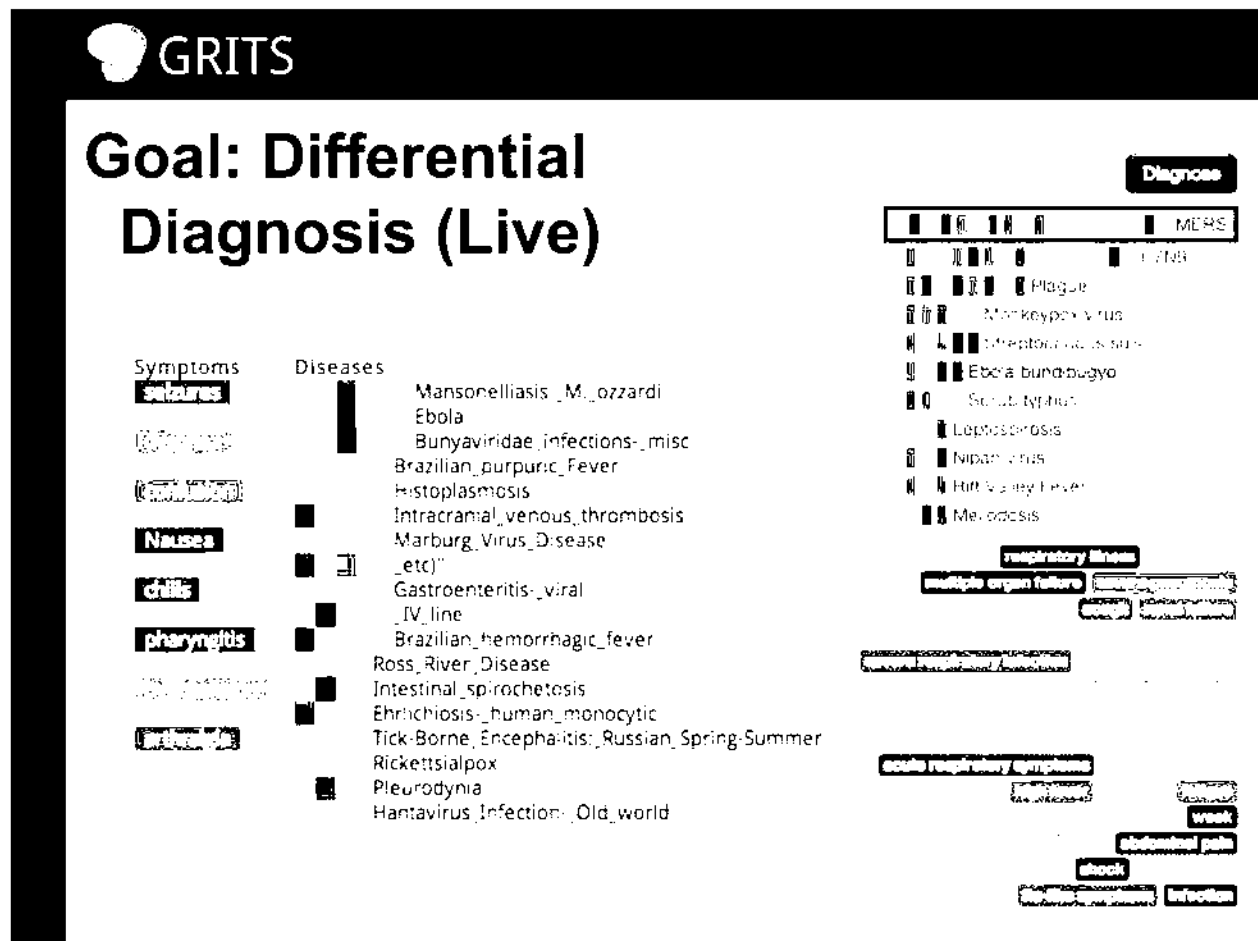


## C. Conceptual diagrams

These slides were presented to DTRA in January to illustrate the goals for GRITS as a service, both via user interface (UI) and application programming interface (API).

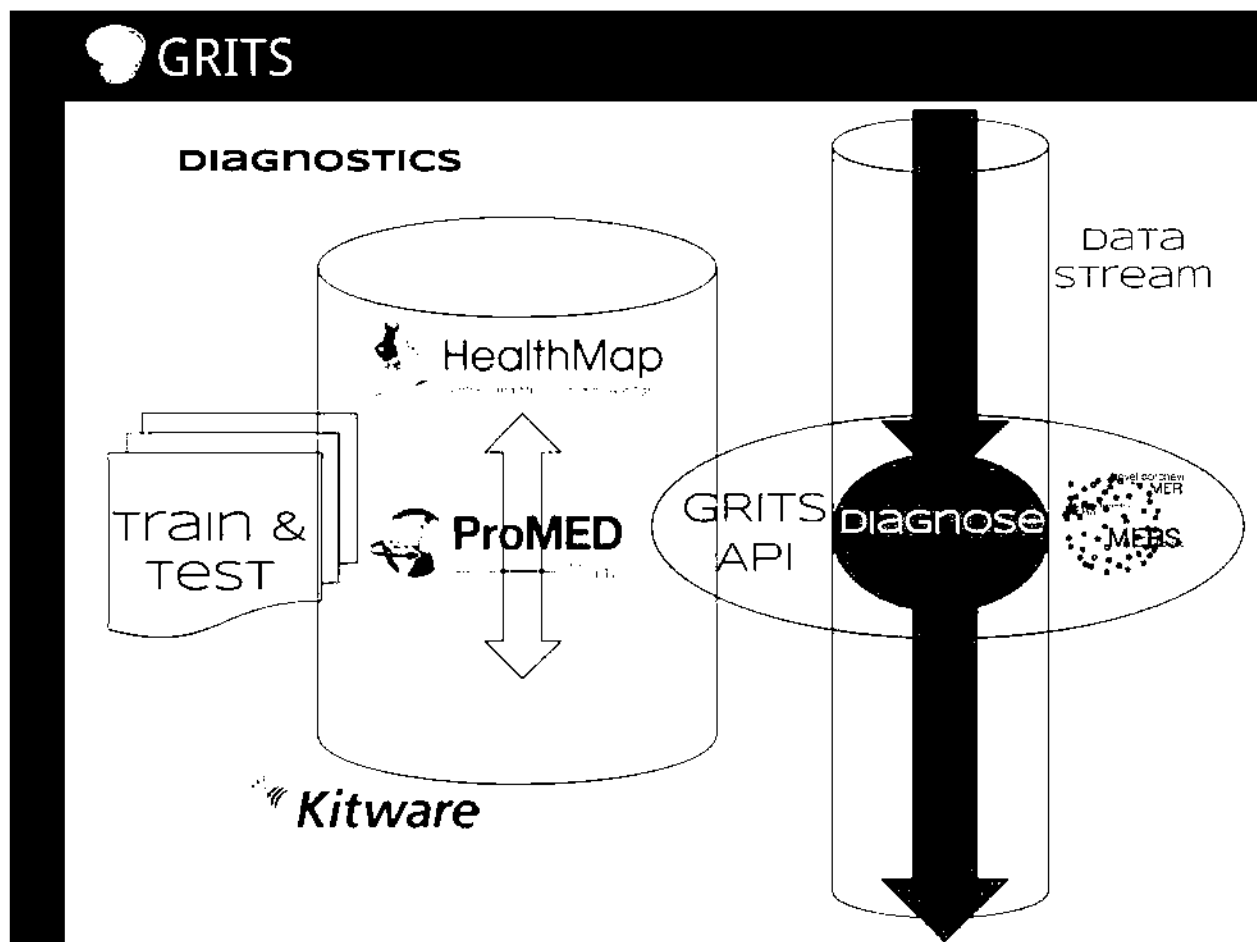
### GRITS.md

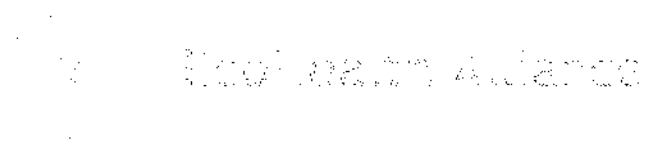
The goal of GRITS.md (v1) was to return ranked differential diagnostics. We developed visualizations in GRITS.app (v1) to display the results of keyword classification (shown as ranked list of results where color matches symptom) and machine learning (shown as black outline for MERS).



## GRITS.md service

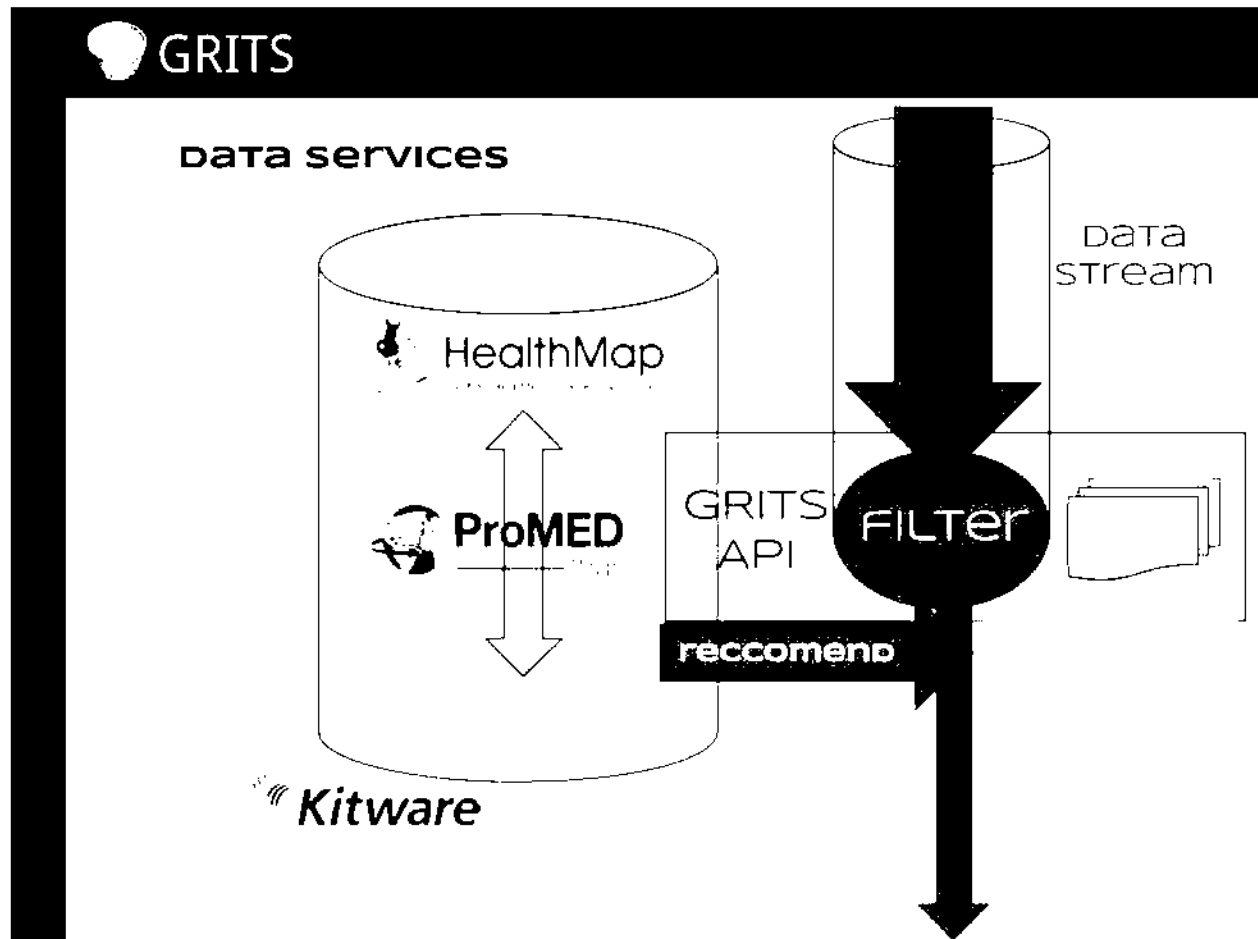
GRITS is designed to eventually be coupled to a high-volume data stream and to diagnose documents in near-real-time. This service will be accessible via the Application Programming Interface (GRITS.api) to diagnose data being ingested or stored in the BSVE or other biosurveillance applications. The diagnostic model is trained and tested on data from Healthmap, ProMED-mail, and EcoHealth Alliance that has been curated by experts via GRITS.app.





## GRITS data services

GRITS is being designed to leverage diagnostics to reduce (filter) a high-volume datastream to relevant resources and recommend related resources from our repositories.



Here are screenshots for some of the tools we demonstrated to DTRA in January.

This is the portfolio interface to GRITS.app to enable expert editors at ProMED-mail, HealthMap, and EHA to curate documents into outbreak portfolios for training the diagnostic tools.



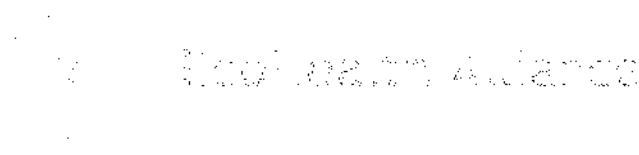
$p_{\text{entr}} = m_{\text{comp}}$

PRO/AMEDR> Ebola hemorrhagic  
fever - Uganda 1993: Bundibugyo.

$$\begin{aligned} \left\{ \begin{array}{l} \text{if } \text{index}^{\text{old}} = \text{index}^{\text{new}} \text{ then } \text{index}^{\text{old}} := \text{index}^{\text{new}} + 1 \\ \text{else } \text{index}^{\text{old}} := \text{index}^{\text{new}} \end{array} \right. \end{aligned}$$

### Export JSON nodes

- ## Diagnosis



## GRITS.app annotator

This is the prototype for the annotation functions of our GRITS.app. This is where expert editors at ProMED-mail, HealthMap, and EHA work together to annotate documents for training the GRITS media diagnostic tools (GRITS.md).

**Ebola bundibugyo (Uganda, 2007)**  
 PRO/A/EBR> Hemorrhagic fever - Uganda (05) (Bundibugyo) Marburg NOT  
 PRO/A/EBR> Hemorrhagic fever - Uganda (04) (Bundibugyo) Ebola confirmed  
 PRO/A/EBR> Ebola hemorrhagic fever - Uganda (Bundibugyo), WHO  
 PRO/A/EBR> Ebola hemorrhagic fever - Uganda (05) (Bundibugyo)  
 PRO/A/EBR> Ebola hemorrhagic fever - Uganda (04) (Bundibugyo)  
 PRO/A/EBR> Ebola hemorrhagic fever - Uganda (05) (Bundibugyo)  
 PRO/A/EBR> Ebola hemorrhagic fever - Uganda (06) (Bundibugyo)  
 PRO/A/EBR> Ebola hemorrhagic fever - Uganda (07) (Bundibugyo), WHO

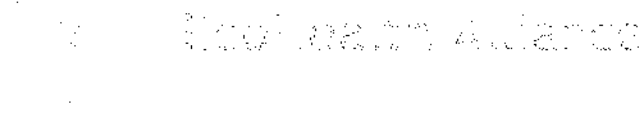
View printable version &nbsp; Share this post: Published Date: 2007-11-16 23:00:00 Subject: PRO/A/EBR>  
 Hemorrhagic fever - Uganda (02) (Bundibugyo), Marburg NOT Archive Number: 20071116.0718  
 HEMORRHAGIC fever - UGANDA (02) (BUNDIBUGYO), MARBURG NOT  
 ..... A ProMED-mail post <http://www.promedmail.org> > ProMED-mail is a program of the International Society for Infectious Diseases <http://www.isid.org> > Date: Fri 16 Nov 2007 Source: The New York Times, Reuters report [edited] [http://www.nytimes.com/reuters/world/international/uganda-fever.html?\\_r=1](http://www.nytimes.com/reuters/world/international/uganda-fever.html?_r=1) > A mysterious fever has killed 14 people and infected 33 others in western Uganda over the last 3 months, a health Ministry official said on Friday (16 Nov 2007). Sam Oware said the fever, though deadly, was not hemorrhagic. Blood samples from it had already tested negative for the killer Marburg virus that infected 3 people in a nearby district in August (2007), killing one. Victims of the fever were found in Uganda's Bundibugyo District, on the border with Democratic Republic of Congo (DRC) and not from the DRC, he said. But from where? because of severe diarrhea. All had complained of fever and abdominal

Info Visualization  
 Geo Visualization  
 Symptom Visualization  
 Diagnose

---

**Resource Tags**  
☒ Review Complete  
 Symptom   
 Add  
 Hide all Reviewed Tags Show all  
**Missing**  
 Hide all Candidate Tags Show all  
**Reject all** symptom   
**Reject all** disease





## E. Visualizations and the Girder database (Kitware)

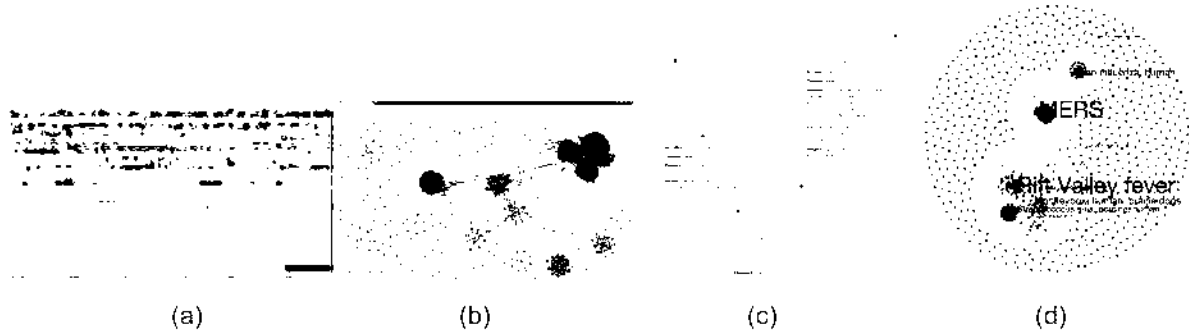


Figure 1. Visualizations provided by Kitware for the GRITS effort. (a) Scatterplot, (b) symptom-country graph view, (c) decision matrix dendrogram, (d) multivariate graph.

In Year 1, Kitware's main deliverables were providing visualizations to the GRITS team, as well as helping to guide the project through discussions of analysis ideas and future directions. Here, we give high-level detail to important contributions.

### Scatterplot visualization

Kitware provided a scatterplot visualization for ProMED mail reports (see Figure 1a). This shows all reports over a 6-month period, representing four dimensions simultaneously (country, time, disease, and number of votes). The view supports interactive filtering by country and disease.

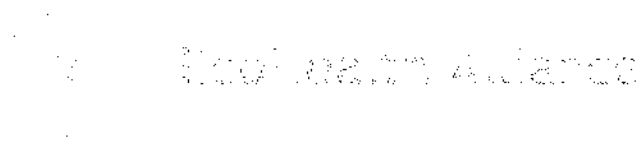
### Symptom-country graph view

In this visualization (see Figure 1b), colored nodes represent diseases, countries, and reports, with an edge appearing between every report and each country and disease that it reports. The network therefore represents possible epidemic situations by clustering countries and diseases by common reports. This graph changes by report date, showing via animation how the epidemic situations may be changing.

### Decision matrix dendrogram

This dendrogram (see Figure 1c) visualizes a symptom/disease matrix, with each internal node representing a symptom, selected to create as even a split as possible between the diseases exhibiting it and those that do not. Each subtree is structured similarly from the remaining symptoms, while leaf nodes represent sets of diseases that cannot be distinguished any further. The diagram displays pop-up information about each node, and supports collapsing of nodes that not interesting to the user.





### **Multivariate graph visualization**

One of the more advanced visualization ideas developed was to create a graph visualization of reports (see Figure 1d) that supports a combination of links from report references, geospatial proximity, and symptom commonality. Also developed in this view is a labeler which dynamically summarizes close nodes to simplify the graphic and highlight the important themes in the data.

### **HealthMap data in GIRDER**

As part of this effort, we also imported a large subset of the HealthMap data into GIRDER, a new open-source tool for data management. In addition to authentication and a flexible back-end storage (MongoDB, Amazon S3, and filesystem), full-text search was implemented to allow instant searchable access to all HealthMap reports.

Pentagon, Room 3C949A

Office: (b)(6)

NIPR

SIPR

<<https://www.linkedin.com/company/dodchembiodefense/>> <<https://www.youtube.com/c/dodchembiodefense>>  
<<https://www.acq.osd.mil/ncbdp/cbd/index.html>>

From: (b)(6)

<mailto:

Sent: Monday, August 15, 2022 2:43 PM

To: (b)(6)

Cc:

>

Subject: FW: PUBLIC HEALTH IMPLICATIONS OF FEDERAL FUNDING PROVIDED FOR CERTAIN  
VIROLOGICAL RESEARCH (OSD010438-21)

(b)(6)

(b)(5)

v/r

(b)(6)

Special Assistant

OASD Legislative Affairs  
Pentagon 3D844

Office: (b)(6)

Cell:

(b)(6)

NIPP

From:

(b)(6)

<mail

Sent: Monday, August 15, 2022 1:15 PM

To:

(b)(6)

<m

(b)(6)

Cc:

(b)(6)

<m

(b)(6)

Subject: RE: PUBLIC HEALTH IMPLICATIONS OF FEDERAL FUNDING PROVIDED FOR CERTAIN  
VIROLOGICAL RESEARCH (OSD010438-21)

Looping in (b)(6) for SA.

From:

(b)(6)

<mail

Sent: Friday, August 12, 2022 12:46

To:

(b)(6)

<m

Cc:

(b)(6)

Subject: FW: PUBLIC HEALTH IMPLICATIONS OF FEDERAL FUNDING PROVIDED FOR CERTAIN  
VIROLOGICAL RESEARCH (OSD010438-21)

\*\*Messaging you because of COL Gillam and CDR Oman's out of office messages.\*\*

(b)(6)

(b)(5)

(b)(6)

in the LA lead for the action.

Respectfully,

(b)(6)

Office of the ASD(A)

Legislative and Congressional Analyst

Pentagon Rm. 3E185

Washington, DC 20301-3600

SIPR: (b)(6)

Office

From:

(b)(6)

Sent: Friday, August 12, 2022 11:56 AM

To: (b)(6)

Cc:

>

Subject: FW: PUBLIC HEALTH IMPLICATIONS OF FEDERAL FUNDING PROVIDED FOR CERTAIN  
VIROLOGICAL RESEARCH (OSD010438-21)

(b)(6)

Who is your Congressional POC in NCB?

Mine was always CDR Oman.

V/r,

(b)(6)

From:

(b)(6)

Sent: Friday, August 12, 2022 11:53 AM

To: (b)(6)

>

Cc:

<m

(b)(6)

>

Subject: FW: PUBLIC HEALTH IMPLICATIONS OF FEDERAL FUNDING PROVIDED FOR CERTAIN  
VIROLOGICAL RESEARCH (OSD010438-21)

(b)(6)

NCB was the OPR for OSD010438-21.

Respectfully,

(b)(6)

From: (b)(6)

<mail

Sent: Friday, August 12, 2022 10:44 AM

To: (b)(6)

<m

Subject: FW: PUBLIC HEALTH IMPLICATIONS OF FEDERAL FUNDING PROVIDED FOR CERTAIN  
VIROLOGICAL RESEARCH (OSD010438-21)

From: (b)(6)

<mail

Sent: Monday, March 7, 2022 16:14

To: (b)(6)

>

Subject: FW: PUBLIC HEALTH IMPLICATIONS OF FEDERAL FUNDING PROVIDED FOR CERTAIN  
VIROLOGICAL RESEARCH (OSD010438-21)

(b)(6)

(b)(5)

V/r,

(b)(6)

From: (b)(6)  
<mail  
Sent: Tuesday, March 1, 2022 12:26 PM  
To: (b)(6)  
>  
<m  
(b)(6)  
Cc: (b)(6)  
<m  
(b)(6)

(b)(6) >, OSD Pentagon OUSD A-S Mailbox  
AS-CMO <osd.pentagon.ousd-a-s.mbx.as-cmo@mail.mil <mailto:osd.pentagon.ousd-a-s.mbx.as-cmo@mail.mil> >  
Subject: PUBLIC HEALTH IMPLICATIONS OF FEDERAL FUNDING PROVIDED FOR CERTAIN  
VIROLOGICAL RESEARCH (OSD010438-21)

All:

Please forward attached Response Letters and Enclosed to Sen Homeland Sec Committees.

V/r

(b)(6)

Executive Correspondence

OUSD (A&S) ECO

Pentagon 3D886

(b)(6)

**From:** (b)(6)  
**To:**  
**Subject:** Fwd: FYSA - WIV and EcoHealth  
**Date:** Friday, April 1, 2022 1:26:14 PM  
**Attachments:** Inside the Virus-Hunting Nonprofit at t...pdf

---

**From:** (b)(6)  
<mailto:(b)(6)>  
**Date:** Friday, April 1, 2022 at 7:06:00 AM  
**To:** (b)(6)

(b)(6)

**Cc:** (b)(6)  
**Subject:** FYSA - WIV and EcoHealth

Sir,

(b)(6) found an article yesterday that I thought we should flag for you.

V/r,

(b)(6)

OASD(NCB/CBD)

Pentagon -- 3C949A

Desk (b)(6)  
Cell:

INVESTIGATION

# “This Shouldn’t Happen”: Inside the Virus-Hunting Nonprofit at the Center of the Lab-Leak Controversy

Chasing scientific renown, grant dollars, and approval from Dr. Anthony Fauci, Peter Daszak transformed the environmental nonprofit EcoHealth Alliance into a government-funded sponsor of risky, cutting-edge virus research in both the U.S. and Wuhan, China. Drawing on more than 100,000 leaked documents, a *NYT* investigation shows how an organization dedicated to preventing the next pandemic found itself suspected of helping start one.

BY KATHERINE EBAN

MARCH 11, 2022





**O**n June 18, 2021, an evolutionary biologist named Jesse D. Bloom sent the draft of an unpublished scientific paper he'd written to Dr. Anthony Fauci, the chief medical adviser to the president of the United States. A bespectacled, boyish-looking 43-year-old often clad in short-sleeved checkered shirts, Bloom specializes in the study of how viruses evolve. "He is the most ethical scientist I know," said Sergei Pond, a fellow evolutionary biologist. "He wants to dig deep and discover the truth."

The paper Bloom had written—known as a preprint, because it had yet to be peer-reviewed or published—contained sensitive revelations about the National Institutes of Health, the federal agency that oversees biomedical research. In the interests of transparency, he wanted Fauci, who helms an NIH subagency, the National Institute of Allergy and Infectious Diseases (NIAID), to see it ahead of time. Under ordinary circumstances, the preprint might have sparked a respectful exchange of views. But this was no ordinary preprint, and no ordinary moment.

More than a year into the pandemic, the genesis of SARS-CoV-2, the virus that causes COVID-19, was still a mystery. Most scientists believed that it had made the leap from bats to humans naturally, via an intermediary species, most likely at a market in Wuhan, China, where live wild animals were slaughtered and sold. But a growing contingent were asking if it could have originated inside a nearby laboratory that is known to have conducted risky coronavirus research funded in part by the United States. As speculation, sober and otherwise, swirled, the NIH was being bombarded by Freedom of Information Act (FOIA) lawsuits. Fauci himself needed a security detail, owing to death threats from conspiracy theorists who believed he was covering up some dark secret.

Bloom's paper was the product of detective work he'd undertaken after noticing that a number of early SARS-CoV-2 genomic sequences mentioned in a published paper from China had somehow vanished without a trace. The sequences, which map the nucleotides that give a virus its unique genetic identity, are key to tracking when the virus emerged and how it might have evolved. In Bloom's view, their disappearance raised the possibility that the Chinese government might be trying to hide evidence about the pandemic's early spread. Piecing together clues, Bloom established that the NIH itself had deleted the sequences from its own archive at the request of researchers in Wuhan. Now, he was hoping Fauci and his boss, NIH director Francis Collins, could help him identify other deleted sequences that might shed light on the mystery.

Bloom had submitted the paper to a preprint server, a public repository of scientific papers awaiting peer review, on the same day that he'd sent a copy to Fauci and Collins. It now existed in a kind of twilight zone: not published, and not yet public, but almost certain to appear online soon.

Collins immediately organized a Zoom meeting for Sunday, June 20. He invited two outside scientists, evolutionary biologist Kristian Andersen and virologist Robert Garry, and allowed Bloom to do the same. Bloom chose Pond and Rasmus Nielsen, a genetic biologist. That it was shaping up like an old-fashioned duel with seconds in attendance did not cross Bloom's mind at the time. But six months after that meeting, he remained so troubled by what transpired that he wrote a detailed account, which *Vanity Fair* obtained.

**Flash Sale Ending Soon**  
**Get 1 year for \$29.99 \$8 + a free tote.**  
**Join now▶**

After Bloom described his research, the Zoom meeting became “extremely contentious,” he wrote. Andersen leapt in, saying he found the preprint “deeply troubling.” If the Chinese scientists wanted to delete their sequences from the database, which NIH policy entitled them to do, it was unethical for Bloom to analyze them further, he claimed. And there was nothing unusual about the early genomic sequences in Wuhan.

Instantly, Nielsen and Andersen were “yelling at each other,” Bloom wrote, with Nielsen insisting that the early Wuhan sequences were “extremely puzzling and unusual.”

Andersen—who'd had some of his emails with Fauci from early in the pandemic publicly released through FOIA requests—leveled a third objection. Andersen, Bloom wrote, “needed security outside his house, and my pre-print would fuel conspiratorial notions that China was hiding data and thereby lead to more criticism of scientists such as himself.”

Fauci then weighed in, objecting to the preprint's description of Chinese scientists “surreptitiously” deleting the sequences. The word was loaded, said Fauci, and the reason they'd asked for the deletions was unknown.

That's when Andersen made a suggestion that surprised Bloom. He said he was a screener at the preprint server, which gave him access to papers that weren't yet public. He then offered to either entirely delete the preprint or revise it “in a way that would leave no record that this had been done.” Bloom refused, saying that he doubted either option was appropriate, “given the contentious nature of the meeting.”

At that point, both Fauci and Collins distanced themselves from Andersen's offer, with Fauci saying, as Bloom recalled it, “Just for the record, I want to be clear that I never suggested you delete or revise the pre-print.” They seemed to know that Andersen had gone too far.

Both Andersen and Garry denied that anyone in the meeting suggested deleting or revising the paper. Andersen said Bloom's account was "false." Garry dismissed it as "nonsense." Sergei Pond, however, confirmed Bloom's account as accurate, after having it read aloud to him. "I don't remember the exact phrasing—I didn't take any notes—but from what you described, that sounds accurate. I definitely felt bad for poor Jesse." He added that the "charged-up" atmosphere struck him as "inappropriate for a scientific meeting." A spokesperson for Fauci declined to comment.

Six months after his contentious meeting with Fauci and other top scientists on June 20, 2021, Jesse Bloom made a written record of his recollections. *Vanity Fair* later obtained the document. [Click here to see and download the full document.](#)

**T**he wagon-circling on that Zoom call reflected a siege mentality at the NIH whose cause was much larger than Bloom and the missing sequences. It couldn't be made to disappear with creative editing or deletion. And it all began with a once-obscure science nonprofit in Manhattan that had become the conduit for federal grant money to a Wuhan research laboratory.

In 2014, Fauci's agency had issued a \$3.7 million grant to EcoHealth Alliance, a nongovernmental organization dedicated to predicting and helping to prevent the next pandemic by identifying viruses that could leap from wildlife to humans. The grant, titled Understanding the Risk of Bat Coronavirus Emergence, proposed to screen wild and captive bats in China, analyze sequences in the laboratory to gauge the risk of bat viruses infecting humans, and build predictive models to examine future risk. The Wuhan Institute of Virology (WIV) was a key collaborator to whom EcoHealth Alliance gave almost \$600,000 in sub-awards. But the work there had been controversial enough that the NIH suspended the grant in July 2020.

As it happened, EcoHealth Alliance failed to predict the COVID-19 pandemic—even though it erupted into public view at the Huanan Seafood Wholesale Market, a short drive from the WIV itself. In the ensuing months, every move of EcoHealth Alliance, and its voluble president Peter Daszak, came under scrutiny by a small army of scientific sleuths and assorted journalists. What, they wanted to know, had really gone on at the WIV? Why had Daszak been so cagey about the work his organization had been funding there? And were Fauci and other officials trying to direct attention away from research that the U.S. had been, at least indirectly, financing?

The dispute over COVID-19's origins has become increasingly acrimonious, with warring camps of scientists trading personal insults on Twitter feeds. Natural-origin proponents argue that the virus, like so many before it, emerged from the well-known phenomenon of natural spillover, jumping from a bat host to an intermediate species before going on to infect humans. Those suspecting a lab-related incident point to an array of possible scenarios, from inadvertent exposure of a scientist during field research to the accidental release of a natural or manipulated strain during laboratory work. The lack of concrete evidence supporting either theory has only increased the rancor. "Everyone is looking for a smoking gun that would render any reasonable doubt impossible," says Amir Attaran, a biologist and lawyer at the University of Ottawa. Without cooperation from the Chinese government, that may be impossible.

In 2018, Daszak had appeared on Chinese state-run TV and said, "The work we do with Chinese collaborators is published jointly in international journals and the sequence data is uploaded onto the internet free for everyone to read, very open, very transparent, and very collaborative." He added, "Science is naturally transparent and open.... You do something, you discover something, you want to tell the world about it. That's the nature of scientists."

But as COVID-19 rampaged across the globe, the Chinese government's commitment to transparency turned out to be limited. It has refused to share raw data from early patient cases, or participate in any further international efforts to investigate the virus's origin. And in September 2019, three months before the officially recognized start of the pandemic, the Wuhan Institute of Virology took down its database of some 22,000 virus samples and sequences, refusing to restore it despite international requests.

As for transparency-minded scientists in the U.S., Daszak early on set about covertly organizing a letter in the *Lancet* medical journal that sought to present the lab-leak hypothesis as a groundless and destructive conspiracy theory. And Fauci and a small group of scientists, including Andersen and Garry, worked to enshrine the natural-origin theory during confidential discussions in early February 2020, even though several of them privately expressed that they felt a lab-related incident was likelier. Just days before those discussions began, *Vanity Fair* has learned, Dr. Robert Redfield, a virologist and the director of the Centers for Disease Control and Prevention (CDC), had urged Fauci privately to vigorously investigate both the lab and natural hypotheses. He was then excluded from the ensuing discussions—learning only later that they'd even occurred. "Their goal was to have a single narrative," Redfield told *Vanity Fair*.

Why top scientists linked arms to tamp down public speculation about a lab leak—even when their emails, revealed via FOIA requests and congressional review, suggest they held similar concerns—remains unclear. Was it simply because their views shifted in favor of a natural origin? Could it have been to protect science from the ravings of conspiracy theorists? Or to protect against a revelation that could prove fatal to certain risky research that they deem

indispensable? Or to protect vast streams of grant money from political interference or government regulation?

The effort to close the debate in favor of the natural-origin hypothesis continues today. In February, *The New York Times* gave front-page treatment to a set of preprints—written by Michael Worobey at the University of Arizona, Kristian Andersen at Scripps Research Institute, and 16 coauthors, including Garry—claiming that a new analysis of public data from the Huanan market in Wuhan provided “dispositive evidence” that the virus first leapt to humans from animals sold there. But a number of top scientists, Bloom among them, questioned that assertion, saying the preprints, while worthy, relied on incomplete data and found no infected animal.

“I don’t think they offer proof. They provide evidence that more strongly supports the link to the wild animal market than to the WIV, and that’s the way I would have phrased it,” says W. Ian Lipkin, an epidemiologist at Columbia University who favors the natural-origin theory.

“Some scientists seem almost hell-bent on naming the Huanan market as the site of the origin of the pandemic; and some members of the media seem more than happy to embrace these conclusions without careful examination,” said Stanford microbiologist David Relman. “This issue is far too important to be decided in the public domain by unreviewed studies, incomplete and unconfirmed data, and unsubstantiated proclamations.”

Perhaps more than anyone, Peter Daszak—a Western scientist immersed in Chinese coronavirus research at the Wuhan Institute of Virology—was uniquely positioned to help the world crack open the origin mystery, not least by sharing what he knew. But last year, Dr. Jeffrey Sachs, the Columbia University economist who oversees the *Lancet*’s COVID-19 commission, dismissed Daszak from the helm of a task force investigating the virus’s genesis, after he flatly refused to share progress reports from his contested research grant. (In written responses to detailed questions, Daszak said he was “simply following NIH guidance” when he declined Sachs’s request, because the agency was withholding the reports in question “until they had adjudicated a FOIA request.” The reports are now publicly available, he said.)

“[Daszak] and NIH have acted badly,” Sachs told *Vanity Fair*. “There has been a lack of transparency...and there is a lot more to know and that can be known.” He said that the NIH should support an “independent scientific investigation” to examine the “possible role” in the pandemic of the NIH, EcoHealth Alliance, the Wuhan Institute of Virology, and a partner laboratory at the University of North Carolina. “Both hypotheses are still very much with us,” he said, and “need to be investigated seriously and scientifically.” (“We are also on record as welcoming independent scientific investigation into the origins of the COVID-19 pandemic,” Daszak told *Vanity Fair*.)

This story is based on more than 100,000 internal EcoHealth Alliance documents obtained by *Vanity Fair*, as well as interviews with five former staff members and 33 other sources. The documents, most of which predate the pandemic, span a number of years and include budgets, staff and board meeting minutes, and internal emails and reports. While the documents do not tell us where COVID-19 came from, they shed light on the world in which EcoHealth Alliance has operated: one of murky grant agreements, flimsy oversight, and the pursuit of government funds for scientific advancement, in part by pitching research of steeply escalating risk.

**T**he story of how Daszak's grant entangled Fauci in the specter of Wuhan coronavirus research began years earlier, at a stately Beaux Arts social club in Washington, D.C. For more than a decade, EcoHealth Alliance hosted a series of cocktail parties at the Cosmos Club near DuPont Circle to discuss the prevention of viral outbreaks. There, expert biologists, virologists, and journalists mingled with the true guests of honor: federal government bureaucrats who were in the position to steer grants.

On invitations, EcoHealth Alliance described the events as “educational.” Inside the nonprofit, however, officials called them “cultivation events.” The return on investment was excellent: For about \$8,000 in Brie and Chardonnay per event, they got to network with prospective federal funders. As the organization's 2018 strategic plan spelled out, “Given our strength in federal funding, we enhanced our cultivation events at the Cosmos Club in Washington DC, which now regularly attract 75-150 people at high levels in govt agencies, NGOs and the private sector.” (“These kinds of events are common among many nongovernmental organizations and nonprofits, which depend upon both public and private donors for support,” Daszak told *Vanity Fair*.)

Of all those high-level people, almost no one ranked as high as Fauci, a scientific kingmaker who dispensed billions in grant money each year—and Daszak was determined to share a podium with him. The idea was admittedly a reach. Though he'd met with Fauci and received funding from his agency, Daszak was relatively obscure. But he had cultivated back-channel access to the minders who guarded Fauci's calendar.

On September 9, 2013, Daszak emailed Fauci's senior adviser David Morens to see if the sought-after NIAID chief would be available as a panel speaker. Morens emailed back, recommending that Daszak “write Tony directly, thanking him for meeting with you all recently and then inviting him to be a member of this Cosmos Club discussion. That way, it is personal and doesn't look ‘cooked’ by us.”

Though Fauci declined that invitation and several others, Daszak kept trying. In February 2016, Morens passed along a valuable tip: Fauci “normally says no to almost everything like this.

Unless ABC, NBC, CBS, and Fox are all there with cameras running. If he were asked to give THE main talk or the only talk that might increase the chances.”

The gambit worked. Fauci signed on to give a presentation on the Zika virus at the Cosmos Club on March 30, and the RSVPs flowed in. The guests came from an array of deep-pocketed federal agencies: the Department of Homeland Security, the U.S. Agency for International Development, the Pentagon, even NASA. As Daszak would declare at a board meeting on December 15, the “Washington, DC cultivation events have been a great way to increase our visibility to federal funders,” according to meeting minutes. A month earlier, Donald Trump had been elected president. One board member at the meeting asked what his incoming administration might mean for a conservation nonprofit dependent on federal grants. Daszak offered breezy reassurance: The organization’s “apolitical mission” would help it adapt.

Little did he know that, in the era of Trump and COVID-19, science itself would become the ultimate political battleground.



EcoHealth Alliance's D.C. "cultivation events," whose guest speakers would include Dr. Anthony Fauci, are said in board meeting minutes to improve "visibility" to federal funders. [Click here](#) to see and download the full document.

f a shared podium with Fauci proved that Daszak had become a true player among virus hunters, it also underscored just how far he had come. For years, Peter Daszak sat at the helm of a struggling nonprofit with a mission to save manatees, promote responsible pet ownership, and celebrate threatened species. The organization, which operated under the name Wildlife Trust until 2010, was constantly on the hunt for ways to close its budget shortfalls. One year, it proposed to honor at its annual benefit a mining company operating in Liberia that was paying it to assess the risks of Ebola virus. Another idea was to seek donations from palm-oil millionaires leveling rainforests who might be interested in “cleaning up” their image.

Balding and usually clad in hiking gear, Daszak was one part salesman, one part visionary. He saw clearly that human incursions into the natural world could lead to the emergence of animal pathogens, with bats a particularly potent reservoir. Daszak was “making a bet that bats were harboring deadly viruses,” said Dr. Matthew McCarthy, an associate professor of medicine at Weill Cornell Medical Center in New York. In 2004, as a 23-year-old Harvard medical student, McCarthy followed Daszak to Cameroon to trap bats. “I left my family, my friends,” he said. “It was a very powerful thing for people like me, going into the most remote parts of the world. I was taken by him, hook, line, and sinker.”

The bioterror attacks of 2001, in which letters dusted with anthrax spores were sent through the U.S. mail, coupled with the first SARS coronavirus outbreak in China the following year, would bring money for the study of lethal natural pathogens pouring into federal agencies. In 2003, the NIAID got an eye-popping \$1.7 billion for research to defend against bioterrorism.

Daszak’s office on Manhattan’s Far West Side didn’t have a laboratory. The closest bat colonies were in Central Park. But he cultivated an affiliation with Shi Zhengli, a Chinese scientist who would rise to become the director of the Wuhan Institute of Virology’s Center for Emerging Infectious Diseases. Slight and sophisticated with an international education, Shi became known in China as “bat woman” for her fearless exploration of their habitats. Daszak’s alliance with her would open China’s bat caves to him.

In 2005, after conducting field research in four locations in China, Daszak and Shi coauthored their first paper together, which established that horseshoe bats were a likely reservoir for SARS-like coronaviruses. They would go on to collaborate on 17 papers. In 2013, they reported their discovery that a SARS-like bat coronavirus, which Shi had been the first to successfully isolate in a lab, might be able to infect human cells without first jumping to an intermediate animal. “[Peter] respected her,” said the former EcoHealth Alliance staffer. “In the view of everyone, they were doing great work for the world.” Their partnership gave Daszak an almost proprietary sense of the bat caves in Yunnan province, which he would later refer to in a grant proposal as “our field test sites.”

As Daszak's staff and Shi's graduate students intermingled, traveling between Wuhan and Manhattan, the exchange flourished. When Shi visited New York, the EcoHealth staff selected a restaurant for a celebratory dinner with great care. "Zhengli is not one to stand on formality; she makes dumplings by hand with her students in the lab!!" Daszak's chief of staff wrote to another employee. "She got her PhD in France, loves red wine, and likes good food above formality."

By 2009, bats had turned into big money. That September, USAID awarded a \$75 million grant called PREDICT to four organizations, including Daszak's. It was "the most comprehensive zoonotic virus surveillance project in the world," USAID stated, and its purpose was to identify and predict viral emergence, in part by sampling and testing bats and other wildlife in remote locations.

The \$18 million over five years awarded to what was then Wildlife Trust was a "game-changer," Daszak told his staff in an ecstatic email sharing the news. "I want to take this opportunity (despite 7 hours of drinking champagne – literally!) to thank all of you for your support."

The money transformed the ragged nonprofit. It increased its budget by half, ending a yearslong operating loss; began a long-deferred rebranding, which led to the new name EcoHealth Alliance; and spruced up its headquarters, even fixing its chronically broken air conditioner. Over the course of the grant, it allocated \$1.1 million to the Wuhan Institute of Virology, USAID recently acknowledged in a letter to Congress.

**W**hen Dr. Maureen Miller, an infectious disease epidemiologist, arrived at EcoHealth Alliance in 2014, she landed in an environment that she found to be toxic and secretive. Closed-door meetings were the norm. The senior leadership constituted an unwelcoming "old boys network." She soon came to believe that she was hired "because they needed a senior-level woman," she said, adding, "I was excluded from pretty much everything."

She came aboard shortly before the organization's PREDICT grant was renewed for five more years. It was also the year the NIH approved Understanding the Risk of Bat Coronavirus Emergence, the \$3.7 million grant that would come back to haunt Fauci. Miller said she was "lured by the idea of being able to create a pandemic-threats warning system."

Miller got to work creating a surveillance strategy to detect zoonotic virus spillover. Chinese villagers living near bat caves in Southern Yunnan province would have their blood tested for antibodies to a SARS-like coronavirus, then answer questionnaires to determine if certain behaviors had led them to be exposed. It was a "biological and behavioral warning system," Miller explained.

Over the next two years, Miller saw Daszak only a handful of times. But she worked closely with Shi Zhengli, who developed the test to screen the villagers' blood. In that time, Miller noted, "I never got a result from [Shi] via phone. I had to show up in China to learn anything from her." From that, Miller gleaned that, while Shi was a "world-class scientist, she respects the Chinese system." In short, she followed the Chinese government's rules. (Shi Zhengli did not respond to written questions for this article.)

Miller left EcoHealth Alliance in November 2016, never knowing what became of the strategy she'd developed. But in the fall of 2017, Shi alerted Miller's former assistant to the fact that Daszak was about to get credit for her work in an upcoming publication. "Shi went out of her way to ensure I would be included," Miller said. The final version of a letter, published in January 2018 in the Wuhan Institute of Virology's journal, *Virologica Sinica*, included Miller's name. Six out of 218 villagers had tested positive for antibodies, suggesting that the strategy was a successful way to gauge potential spillover.

But the experience left Miller with a dark impression of Daszak: "He is so single-minded that he wants to be the one who makes the discovery, without having to share."

Daszak said Miller has been credited as a coauthor on at least eight papers stemming from her work at EcoHealth Alliance, "a testimony to the equity, fairness, and openness of our publication and authorship practices." He added that the nonprofit's staff is "diverse and culturally sensitive" and has been "majority female for 20 years."

**D**aszak's \$3.7 million NIH grant first set off alarm bells in early May 2016, as it entered its third year. The NIH requires annual progress reports, but Daszak's year-two report was late and the agency threatened to withhold funds until he filed it.

The report he finally did submit worried the agency's grant specialists. It stated that scientists planned to create an infectious clone of Middle East Respiratory Syndrome (MERS), a novel coronavirus found in dromedaries that had emerged in Saudi Arabia in 2012 and killed 35% of the humans it infected. The report also made clear that the NIH grant had already been used to construct two chimeric coronaviruses similar to the one that caused Severe Acute Respiratory Syndrome (SARS), which emerged in 2002 and went on to cause at least 774 deaths worldwide. (A chimeric virus is one that combines fragments of different viruses.) These revelations prompted the NIH's grant specialists to ask a critical question: Should the work be subject to a federal moratorium on what was called gain-of-function research?

With that, Daszak's grant got tangled in a yearslong debate that had divided the virology community. In 2011, two scientists separately announced that they had genetically altered

Highly Pathogenic Asian Avian Influenza A (H5N1), the bird flu virus that has killed at least 456 people since 2003. The scientists gave the virus new functions—enabling it to spread efficiently among ferrets, which are genetically closer to humans than mice—as a way to gauge its risks to people. Both studies had received NIH funding.

The scientific community erupted in conflict over what became known as gain-of-function research. Proponents claimed it could help prevent pandemics by highlighting potential threats. Critics argued that creating pathogens that didn't exist in nature ran the risk of unleashing them. As the dispute raged, Fauci worked to strike a middle ground, but ultimately supported the research, arguing in a coauthored *Washington Post* op-ed that “important information and insights can come from generating a potentially dangerous virus in the laboratory.”

In October 2014, the Obama administration imposed a moratorium on new federal funding for research that could make influenza, MERS, or SARS viruses more virulent or transmissible, while a review took place. But the moratorium, as written, left loopholes, which allowed Daszak to try to save the research. On June 8, 2016, he wrote to the NIH's grant specialists that the SARS-like chimeras from the completed experiment were exempt from the moratorium, because the strains used had not previously been known to infect humans. He also pointed to a 2015 research paper in which scientists had infected humanized mice with the same strains, and found that they were less lethal than the original SARS virus.

But the 2015 research paper he cited was not particularly reassuring. In it, Shi Zhengli and a preeminent coronavirus researcher at the University of North Carolina, Ralph Baric, mixed components of SARS-like viruses from different species, and created a novel chimera that was able to directly infect human cells. (Baric did not respond to written questions seeking comment.)

This gain-of-function experiment, which had begun prior to the moratorium, was so fraught that the authors flagged the dangers themselves, writing, “scientific review panels may deem similar studies...too risky to pursue.” The paper's acknowledgments cited funding from the NIH and from EcoHealth Alliance, through a different grant.

If anything, the MERS study Daszak proposed was even riskier. So he pitched a compromise to the NIH: that if any of the recombined strains showed 10 times greater growth than a natural virus, “we will immediately: i) stop all experiments with the mutant, ii) inform our NIAID Program Officer and the UNC [Institutional Biosafety Committee] of these results and iii) participate in decision making trees to decide appropriate paths forward.”

This mention of UNC brought a puzzled response from an NIH program officer, who pointed out that the proposal had said the research would be performed at the WIV. “Can you clarify where

the work with the chimeric viruses will actually be performed?” the officer wrote. Ten days later, with still no response from Daszak, the program officer emailed him again. On June 27, Daszak responded, buoyant as ever:

---

*“You are correct to identify a mistake in our letter. UNC has no oversight of the chimera work, all of which will be conducted at the Wuhan Institute of Virology.... We will clarify tonight with Prof. Zhengli Shi exactly who will be notified if we see enhanced replication...my understanding is that I will be notified straight away, as [principal investigator], and that I can then notify you at NIAID. Apologies for the error!”*

By July 7, the NIH agreed to Daszak’s terms, which relied entirely on mutual transparency: Shi would inform him of any concerning developments involving the lab-constructed viruses, and he would inform the agency. Daszak replied enthusiastically to a program officer, “This is terrific! We are very happy to hear that our Gain of Function research funding pause has been lifted.”

Allowing such risky research to go forward at the Wuhan Institute of Virology was “simply crazy, in my opinion,” says Jack Nunberg, director of the Montana Biotechnology Center. “Reasons are lack of oversight, lack of regulation, the environment in China,” where scientists who publish in prestigious journals get rewarded by the government, creating dangerous incentives. “So that is what really elevates it to the realm of, ‘No, this shouldn’t happen.’”

A subsequent development seemed to support that view. On January 15, 2021, in the waning days of the Trump administration, the State Department released a fact sheet based on declassified intelligence. It asserted that Chinese military scientists had been collaborating with the WIV’s civilian scientists since 2017, if not earlier. That raised the question of whether research there was being repurposed for offensive or military uses. Though Shi and other WIV leaders have previously denied such collaboration occurred, former deputy national security adviser Matthew Pottinger calls those denials “willful lies. If one were to give them the benefit of the doubt, you might go so far as to say they have no choice but to lie, but these are lies nonetheless.”

If China’s military had been collaborating with WIV scientists, it’s unclear if Daszak would have realized it. He had far less visibility into the WIV than he let on, a former EcoHealth Alliance staffer told *Vanity Fair*. The work being done there was “always an enigma,” the former staffer said. The nonprofit had hired a U.S.-based Chinese national who helped “interpret for them what was happening inside the WIV.... But we had to take everything at face value. It was more, ‘Accept what it is, because of this relationship’” between Shi and Daszak.

“He doesn’t know what happened in that lab,” said the former staffer. “He cannot know that.”

According to Daszak, EcoHealth Alliance “was aware” of the WIV’s research activities related to its NIH grant. He says he had no knowledge of Chinese military involvement there and was never notified of any by the U.S. government.

**B**y 2017, despite massive infusions of grant money, EcoHealth Alliance faced a brewing financial crisis. Ninety-one percent of its funding came from the federal government, and 71% of that came from the PREDICT grant, according to minutes of the organization’s finance committee meeting. The renewed grant, known as PREDICT II, was slated to end in two years. There was no way to know if the grant would be reauthorized for a third time. The looming possibility that it would expire came to be known internally as the “PREDICT cliff.”

How to prevent the organization from tumbling over it consumed meeting after meeting. One possible solution was the Global Virome Project, a nongovernmental initiative being organized by the infectious disease specialist Dennis Carroll, who had established PREDICT while working at USAID. The Global Virome Project was far more ambitious: Its goal was to map every possible virus on earth—an estimated 840,000 of which might infect human beings—as a way to “end the pandemic era.”

The program had a steep projected price tag of \$3.4 billion over 10 years, Daszak explained to board members. But the cost of not knowing and suffering a pandemic was estimated at \$17 trillion over 30 years. Looked at that way, the Global Virome Project was a relative bargain.

But there was another way that EcoHealth Alliance could ward off the \$8 million shortfall it was facing. The Defense Department could serve as a federal life raft in a new ocean of grants. The Defense Advanced Research Projects Agency (DARPA) was seeking proposals for a new program called PREEMPT, which aimed to identify animal pathogens “to preempt their entry into human populations before an outbreak occurs.”

For EcoHealth Alliance, the PREEMPT grant seemed like a slam dunk. For years, Daszak had been developing a method of predictive modeling to identify likely sites of viral spillover around the world and stop pandemics at the source. Some questioned the effectiveness of Daszak’s approach. “In 20 years of using this method, [EcoHealth Alliance] did not predict a single outbreak, epidemic or pandemic,” Maureen Miller told *Vanity Fair*. But David Morens, senior adviser to the NIAID director, said that Daszak became one of the “key players” in understanding that “emerging diseases came from animals, the animals had their own geographic ranges, and if you knew where the animals were and what diseases they carried, you could predict hot spots.”

EcoHealth Alliance also doubled down on another key selling point: Its unique on-the-ground connections in China would effectively give the U.S. government a foothold in foreign

laboratories. As Daszak had told his staff at a meeting some years earlier, one Defense Department subagency wanted “information on what is going on in countries in which they cannot access (China, Brazil, Indonesia, India).”

With the PREDICT cliff and the DARPA deadline coming ever closer, Daszak struck an upbeat note with his board, pointing out that the organization had a strong track record of winning federal grants. “This was the golden ticket,” a former staffer familiar with the DARPA grant application said. “The message was always, ‘We are going to do cool and cutting-edge science. DARPA is the right agency to fund this.’”

**L**ast September, EcoHealth Alliance’s grant proposal to DARPA was leaked to DRASTIC, a loosely affiliated global group of sleuths—ranging from professional scientists to amateur data enthusiasts—dedicated to investigating the origins of COVID-19. From the 75-page proposal, a striking detail stood out: a plan to examine SARS-like bat coronaviruses for furin cleavage sites and possibly insert new ones that would enable them to infect human cells.

A furin cleavage site is a spot in the surface protein of a virus that can boost its entry into human cells. SARS-CoV-2, which emerged more than a year after the DARPA grant was submitted, is notable among SARS-like coronaviruses for having a unique furin cleavage site. This anomaly has led some scientists to consider whether the virus could have emerged from laboratory work gone awry.

Documents obtained by *Vanity Fair* shed new light on the chaotic process surrounding the DARPA proposal, which was cocreated with colleagues including Shi Zhengli at the WIV and Ralph Baric at the University of North Carolina at Chapel Hill. As the March deadline approached, the grant’s collaborators worked 24/7, with versions pouring in from around the world. “Those documents were being written by many, many people,” one former employee recalled.

The grant application proposed to collect bat samples from caves in Yunnan Province, transport them to the Wuhan Institute of Virology, extract and manipulate the viruses they contain, and use them to infect mice with humanized lungs. It would then map high-risk areas for bats harboring dangerous pathogens and treat test caves with substances to reduce the amount of virus they were shedding.

It was a long way from saving manatees from motorboats.

By almost any definition, this was gain-of-function research. The federal moratorium had been lifted in January 2017 and replaced with a review system called the HHS P3CO Framework (for



Potential Pandemic Pathogen Care and Oversight). This required a safety review by the agency funding the research.

EcoHealth Alliance's DARPA proposal asserted that its research was exempt from the P3CO framework. It also emphasized the extensive experience of the team it would assemble. But at a staff meeting on March 29, Daszak expressed dismay at the slapdash and amateur nature of the DARPA submission. It was a "major failure on all accounts," he noted, enumerating a cascade of mistakes: The application was late, sent in "30 minutes after deadline." There were errors uploading documents, comment boxes that remained on the pages, a question of who was in charge. What was needed, he exhorted his staff, was a "change in culture" as "part of [a] mentality [sic] to get money," according to the meeting minutes.

EcoHealth Alliance's controversial rejected DARPA grant proposal is described as a "major failure" in staff meeting minutes. [Click here to see and download the document.](#)

Inside DARPA, the grant application was met with immediate skepticism. The contract was “never awarded because of the horrific lack of common sense” it reflected, said a former DARPA official who was there at the time. EcoHealth Alliance was viewed as a “ragtag group” and a “middle guy,” a backseat collaborator willing to get on an Air China jet, eat terrible food, and stay in bad hotels, said the former official.

Likewise, the WIV was also viewed as subpar, especially when compared with the Harbin Veterinary Research Institute, which operated China’s only other high-containment laboratory with the highest biosafety protocol: BSL-4. Harbin was China’s Harvard, said the former DARPA official. The WIV was more like a safety school. EcoHealth Alliance had “bolted on” a serious scientist, Ralph Baric, and “podged” the proposal together. Having the nonprofit serve as the prime contractor for a global project with national security risks was like “having your rental car agency trying to run an armada,” said the former DARPA official.

Though two of three DARPA reviewers deemed it “selectable,” the third, a program manager in the Biological Technologies Office, recommended against funding it. He wrote that the application did not adequately mention or assess the gain-of-function risk or the possibility that the proposed work could constitute dual-use research of concern (DURC), the technical term for science that can be repurposed to cause harm or endanger security.

The DARPA proposal was “basically a road map to a SARS-CoV-2-like virus,” says virologist Simon Wain-Hobson, who is among the scientists calling for a fuller investigation of COVID-19’s origins. If the research had the blessing of a top coronavirus scientist like Baric, then it is possible the WIV would have wanted to copy what it viewed as cutting-edge science, he said. “That doesn’t mean they did it. But it means it’s legitimate to ask the question.”

According to Daszak, no one at DARPA expressed any concerns about the proposed research to EcoHealth Alliance. On the contrary, he said, “DARPA told us that ‘we had a strong proposal’ and ‘wished DARPA had greater funding for the PREEMPT program.’” He added, “the research was never done by EHA or, to my knowledge, any of the collaborating partners on that proposal.”

**B**y late December 2019, cases of what would soon be identified as SARS-CoV-2 began emerging around the Huanan Seafood Wholesale Market in the Jiangnan district of Wuhan, roughly eight miles from the Wuhan Institute of Virology.

Daszak seemed poised to play a leading role in the emerging crisis. On January 2, 2020, he tweeted: “The GOOD news!! is that leading scientists from the US, China and many other countries are working together to actively block the ability of these viruses to spillover, and to rapidly detect them if they do.” He continued, “This includes active collaboration with China

CDC, Wuhan Inst. Virology, @DukeNUS, @Baric\_Lab, and a diverse array of Provincial CDCs, universities and labs across S. and Central China.”

On January 30, Daszak went on CGTN America, the U.S. outpost for Chinese state television, and said two things that proved to be spectacularly wrong. “I’m very optimistic...that this outbreak will begin to slow down,” he said. “We’re seeing a small amount of human-to-human transmission in other countries, but it’s not uncontrollable.” He went on to conclude that the Chinese government was taking all necessary steps “to be open and transparent, and work with WHO, and talk to scientists from around the world, and where necessary, bring them in to help. They’re doing that. It’s exactly what needs to happen.”

In fact, the opposite was true. The virus was spreading uncontrollably and the Chinese government was busy crushing anyone who spoke out: It ordered laboratory samples destroyed, punished doctors who raised alarms, and claimed the right to review any scientific research about COVID-19 ahead of publication, a restriction that remains in place today.

At the highest levels of the U.S. government, alarm was growing over the question of where the virus had originated and whether research performed at the WIV, and funded in part by U.S. taxpayers, had played some role in its emergence.

To Dr. Robert Redfield, the director of the CDC at the time, it seemed not only possible but likely that the virus had originated in a lab. “I personally felt it wasn’t biologically plausible that [SARS CoV-2] went from bats to humans through an [intermediate] animal and became one of the most infectious viruses to humans,” he told *Vanity Fair*. Neither the 2002 SARS virus nor the 2012 MERS virus had transmitted with such devastating efficiency from one person to another.

What had changed? The difference, Redfield believed, was the gain-of-function research that Shi and Baric had published in 2015, and that EcoHealth Alliance had helped to fund. They had established that it was possible to alter a SARS-like bat coronavirus so that it would infect human cells via a protein called the ACE2 receptor. Although their experiments had taken place in Baric’s well-secured laboratory in Chapel Hill, North Carolina, who was to say that the WIV had not continued the research on its own?

In mid-January of 2020, *Vanity Fair* can reveal, Redfield expressed his concerns in separate phone conversations with three scientific leaders: Fauci; Jeremy Farrar, the director of the U.K.’s Wellcome Trust; and Tedros Adhanom Ghebreyesus, director general of the World Health Organization (WHO). Redfield’s message, he says, was simple: “We had to take the lab-leak hypothesis with extreme seriousness.”

It is not clear whether Redfield’s concerns are what sparked Fauci’s own. But on Saturday night, February 1, at 12:30 a.m., Fauci emailed the NIAID’s principal deputy director, Hugh

Auchincloss, under the subject line “IMPORTANT.” He attached the 2015 paper by Baric and Shi and wrote, “Hugh: It is essential that we speak this AM. Keep your cell phone on.” He instructed Auchincloss to read the attached paper and added, “You will have tasks today that must be done.”

February 1 proved to be a critical day. With the death count in China passing 300 and cases popping up in more than a dozen countries, Farrar convened a group of 11 top scientists across five time zones. That morning, he asked Fauci to join. “My preference is to keep this group really tight,” Farrar wrote. “Obviously ask everyone to treat in total confidence.” Fauci, Francis Collins, Kristian Andersen, and Robert Garry all joined the call. No one invited Redfield, or even told him it was happening.

In the conference call and emails that followed over the next four days, the scientists parsed the peculiarities of SARS-CoV-2’s genomic sequence, paying special attention to the furin cleavage site.

Dr. Michael Farzan, an immunologist, emailed the group, writing that the anomaly could result from sustained interaction between a chimeric virus and human tissue in a laboratory that lacked appropriate biocontainment protocols, “accidentally creating a virus that would be primed for rapid transmission between humans.” He leaned toward the lab-origin hypothesis, saying, “I think it becomes a question of...whether you believe in this series of coincidences, what you know of the lab in Wuhan, how much could be in nature—accidental release or natural event? I am 70:30 or 60:40.”

He was not alone. Garry wrote of the “stunning” composition of the furin cleavage site: “I really can’t think of a plausible natural scenario where you get from the bat virus or one very similar to it to [SARS-CoV-2] where you insert exactly 4 amino acids 12 nucleotide[s] that all have to be added at the exact same time to gain this function.... I just can’t figure out how this gets accomplished in nature.”

The previous evening, Andersen had emailed Fauci, saying that he and scientists including Garry, Farzan, and the Australian virologist Edward Holmes all found the genetic sequence “inconsistent with expectations from evolutionary theory.”

But within three days, four of the scientists on the call, including Andersen, Garry, and Holmes, had shared the draft of a letter arguing the opposite. Farrar shared a copy with Fauci, who offered feedback ahead of its publication on March 17 in *Nature Medicine*. The letter, The Proximal Origin of SARS-CoV-2, analyzed the genomic sequence and made a seemingly unequivocal statement: “we do not believe that any type of laboratory-based scenario is plausible.”

How they arrived at such certainty within four days remains unclear. In his book *Spike: The Virus vs. The People—the Inside Story*, Farrar cited “the addition of important new information, endless analyses, intense discussions and many sleepless nights.” But even as they circulated the draft on February 4, qualms remained. Farrar wrote to Collins and Fauci that, while Holmes now argued against an engineered virus, he was still “60-40 lab.”

A Wellcome spokesman told *Vanity Fair*, “Dr. Farrar is in regular conversation with and regularly convenes many other expert scientists.” He added, “Dr. Farrar’s view is that there was at no stage any political influence or interference during these conversations, or in the research carried out.” Garry said that it was “frankly tiresome to explain for the umpteenth time that that was one email cherry-picked among dozens, even hundreds, in part of an ongoing scientific discussion.”

Though he wasn’t part of those conversations, the epidemiologist W. Ian Lipkin told *Vanity Fair*, “I have known Fauci for 30 years. Fauci is not interested in anything but the truth. Anyone that says anything otherwise doesn’t know him.”

Lipkin was added as a fifth author on the Proximal Origin letter. Ahead of publication, he told his coauthors he was concerned that gain-of-function research on coronaviruses was being performed in laboratories with insufficient safeguards. The Proximal Origin letter addresses that issue, but dismisses a possible accident as the source of SARS-CoV-2. Lipkin was not invited to participate in future publications with the group, such as the preprints by Andersen and Worobey that made it onto the front page of *The New York Times* in February. “I can speculate on why I’ve not been asked to join various publications. However, I don’t know why I’ve not been asked,” he said.

While Andersen and the others were fine-tuning the Proximal Origin letter, Daszak was quietly working to bury speculation of a lab leak. On February 19, in a letter published in the influential medical journal *The Lancet*, he joined 26 scientists in asserting, “We stand together to strongly condemn conspiracy theories suggesting that COVID-19 does not have a natural origin.” Nine months later, emails released by a Freedom of Information group showed that Daszak had orchestrated the *Lancet* statement with the intention of concealing his role and creating the impression of scientific unanimity.

Under the subject line, “No need for you to sign the ‘Statement’ Ralph!!,” he wrote to Baric and another scientist: “you, me and him should not sign this statement, so it has some distance from us and therefore doesn’t work in a counterproductive way.” Daszak added, “We’ll then put it out in a way that doesn’t link it back to our collaboration so we maximize an independent voice.”

Baric agreed, writing back, “Otherwise it looks self-serving and we lose impact.”

The *Lancet* statement ended with a declaration of objectivity: “We declare no competing interests.” Among its signatories were Jeremy Farrar and one other participant in the confidential huddle with Fauci.

Reading the *Lancet* letter, with Farrar’s name attached to it, Redfield had a dawning realization. He concluded there’d been a concerted effort not just to suppress the lab-leak theory but to manufacture the appearance of a scientific consensus in favor of a natural origin. “They made a decision, almost a P.R. decision, that they were going to push one point of view only” and suppress rigorous debate, said Redfield. “They argued they did it in defense of science, but it was antithetical to science.”

A Wellcome spokesperson told *Vanity Fair*, “The letter was a simple statement of solidarity with highly reputable researchers based in China and against non-evidence-based theories. Dr. Farrar does not believe the letter was covertly organized. He had no conflict of interest to declare.”

**A**s the pandemic spread to every corner of the globe, Daszak continued to devote his considerable energies to promoting the idea that science itself had reached consensus: The virus emerged from nature, not a lab. But as one concerning detail after another slipped into public view, the facade of unanimity began to crack, exposing his own work to questions.

During a White House COVID-19 press briefing on April 17, 2020, a reporter for the right-wing television network Newsmax asked President Trump why the NIH would fund a \$3.7 million grant to a high-level lab in China. The details were wrong, and the question seemed queued-up to feed an anti-China political agenda. Trump responded, “We will end that grant very quickly.”

That exchange, in turn, uncorked a question from another reporter to Fauci: Could SARS-CoV-2 have come from a lab? His answer from the White House podium was swift and clear. A recently published analysis from a “group of highly qualified evolutionary virologists” had concluded that the virus was “totally consistent with a jump of a species from an animal to a human.” He was referring to the Proximal Origin letter, drafted by some of the scientists he’d met with confidentially in early February.

The next day, Daszak sent an email of profuse thanks to Fauci for “publicly standing up and stating that the scientific evidence supports a natural origin for COVID-19 from a bat-to-human spillover, not a lab release from the Wuhan Institute of Virology.” Fauci responded, thanking him back.

If Daszak thought that Fauci’s kind words meant his grant was safe, he was mistaken. Six days later, he received a sharply worded letter from a senior NIH official: His bat coronavirus

research grant, which had provided subgrants to the WIV, was being terminated. Amid an uproar and legal threats, the agency reinstated the grant several months later, but suspended its activities. So began a bitter, ongoing battle between Daszak and the NIH over whether he'd complied with the grant's terms. Swaths of this private correspondence have become public since last September, as part of a FOIA lawsuit waged by The Intercept.

Daszak also found himself answering increasingly pointed questions about the WIV's decision to take down its online database of 22,000 genomic sequences in September 2019, prior to the known onset of the pandemic.

Maureen Miller says the human blood samples that were collected in China as part of the surveillance strategy she designed at EcoHealth Alliance could hold clues to COVID-19's provenance. But they went into the WIV and are now out of reach. Why would a database supported by U.S. tax dollars to help prevent and respond to a pandemic be made "inaccessible exactly when it was needed to fulfill its intended purpose?" asks Jamie Metzl, a senior fellow at the Atlantic Council, who was among the first to call for a full investigation of COVID-19's origins.

Presumably, Daszak possessed a great deal of that inaccessible data. He said as much during a March 2021 panel organized by a London-based think tank: "A lot of this work has been conducted with EcoHealth Alliance.... We do basically know what's in those databases." Previously, EcoHealth Alliance had signed a pledge, along with 57 other scientific and medical organizations, to share data promptly in the event of a global public health emergency. And yet, in the face of just such an emergency, Daszak told *Nature* magazine, "We don't think it's fair that we should have to reveal everything we do."

In April 2020, he warned colleagues from other institutions that partnered on the PREDICT grants not to publicly release certain sequences. "All - It's extremely important that we don't have these sequences as part of our PREDICT release to Genbank at this point," he wrote. "As you may have heard, these were part of a grant just terminated by NIH. Having them as part of PREDICT will [bring] very unwelcome attention to" the PREDICT program, grant partners, and USAID.

By October 2021, the NIH had repeatedly demanded that EcoHealth Alliance turn over data related to its grant research with the WIV. Daszak argued that he couldn't share a number of SARS coronavirus sequences because he was waiting for the Chinese government to authorize their release. The explanation seemed to undercut the entire rationale for having the U.S. government help fund a global collaboration on virus emergence.

Daszak said it was “incorrect” to suggest that EcoHealth Alliance had not “readily shared data,” and asserted that all of its relevant coronavirus data from NIH-supported research at the WIV has now been made public. He added that he warned about “unwelcome attention” because he wanted “to avoid [colleagues] being dragged into the political fray unfairly” after the NIH’s decision to terminate EcoHealth Alliance’s grant “unleashed a torrent of unwarranted political attacks.”

**U**S. officials and at least one of Daszak’s former colleagues were stunned when, in November 2020, the WHO announced the names of 11 international experts assigned to a fact-finding mission to China to investigate COVID-19’s origins. China had veto power over the list, and none of the three candidates put forward by the U.S. had made the cut. Instead, Peter Daszak was listed as America’s sole representative.

It’s still unclear how Daszak wound up on the commission. “I didn’t want to go, and I said no initially,” he later told *Science* magazine, before adding, “If you want to get to the bottom of the origins of a coronavirus outbreak in China, the number one person you should be talking to is the person who works on coronaviruses in China, who’s not from China.... So that’s me, unfortunately.”

Daszak told *Vanity Fair*, “WHO reached out to me and asked me to serve on the committee. I initially refused, but...following their persuasive arguments decided that it was my duty as a scientist to support the origins investigation.” A WHO spokesperson would neither confirm nor deny Daszak’s account.

One former EcoHealth staffer thinks it’s obvious who tapped Daszak for the role: “If his name was not among the names floated [by the U.S.], his was the name that the Chinese government chose.”

In China, the experts spent half of their monthlong mission quarantined in hotels. Once released, they made one trip to the Wuhan Institute of Virology. Daszak later described the visit to *60 Minutes*: “We met with them. We said, ‘Do you audit the lab?’ And they said, ‘Annually.’ ‘Did you audit it after the outbreak?’ ‘Yes.’ ‘Was anything found?’ ‘No.’ ‘Do you test your staff?’ ‘Yes.’ No one was—”

The correspondent, Lesley Stahl, interrupted: “But you’re just taking their word for it.” Daszak responded, “Well, what else can we do? There’s a limit to what you can do and we went right up to that limit. We asked them tough questions.... And the answers they gave, we found to be believable—correct and convincing.”



On March 24, 2021, Daszak presented a confidential preview of the WHO mission's findings to a group of federal health and national security officials in a packed government conference room. Dressed in a tweed jacket instead of his usual hiking gear, he clicked through a 36-slide presentation, which *Vanity Fair* obtained.

Peter Daszak's 36-slide presentation summarizing the deliberations of the WHO-convened study on COVID-19's origins. [Click here to see and download the full presentation.](#)

Amid the charts, graphs, and old photos from the Huanan market of caged animals that could have harbored the virus, there was one slide devoted to the Wuhan Institute of Virology. It seemed to suggest that the questions swirling around the laboratory as a possible source of the pandemic could be put to rest. There had been annual external audits with no unusual findings.

Access was strictly controlled. And his trusted partner Shi Zhengli said there had been no COVID-like illnesses among her staff.

The presentation complete, Daszak held up his hands, as if waiting for a standing ovation, the attendee recounted: “His ego couldn’t fit in the room with all those interagency partners.”

The WHO Commission released its 120-page final report a week later. The experts had voted, by a show of hands, that direct transmission from bat to human was possible to likely; transmission through an intermediate animal was likely to very likely; transmission through frozen food was possible; and transmission through a laboratory incident was “extremely unlikely.”

The report was so error-riddled and unpersuasive that WHO director general Tedros effectively disowned it the day it was released. “As far as WHO is concerned all hypotheses remain on the table,” he said.

Three months later, the commission’s lead expert, Danish food scientist Peter Ben Embarek, extinguished the last embers of the report’s credibility. He confessed to a documentary film crew that the group had made a backroom deal with the 17 Chinese experts attached to the commission: The report could mention the lab-leak theory only “on the condition we didn’t recommend any specific studies to further that hypothesis” and used the phrase “extremely unlikely” to characterize it.

But that wasn’t the final shoe to drop. Daszak himself all but admitted—in a letter to Dr. Michael Lauer, the NIH’s deputy director for extramural research—that he had signed on to the WHO mission with a personal and professional agenda: to gather exculpatory information about the WIV, in part to help lift the curtain of suspicion around his grant so it could be reinstated.

“I have made extensive efforts to satisfy NIH’s broad concerns,” he wrote on April 11, 2021. “This includes serving as an expert on the WHO-China joint Mission on the Animal Origins of COVID-19, which involved 1 month on the ground in China (including 2 weeks locked in quarantine), at great personal burden and risk to me, to our organization, and to my family.”

He wrote that, while he had “acted in good faith” to follow the WHO’s directives for the mission, he had also gathered essential information that “specifically addresses” one of the demands the NIH had made as a condition of reinstating the grant: that he arrange for an outside inspection team to find out if the WIV had SARS-CoV-2 in its possession prior to December 2019. He’d returned with “categorical statements from WIV senior staff” that they did not have it prior to December 2019, he wrote, and had managed to get their assurances included in the WHO final report.

Unfortunately for Daszak, the NIH was unmoved. The grant remains suspended today.

**O**n February 25, 2022, a day before Worobey, Andersen, Garry, and their 15 coauthors rushed their preprints into the public domain, claiming “dispositive evidence” that SARS-CoV-2 originated from the Huanan market, China’s CDC published a preprint of its own that contained new data and pointed to a different conclusion. It revealed that, of the 457 swabs taken from 18 species of animals in the market, none contained any evidence of the virus. Rather, the virus was found in 73 swabs taken from around the market’s environment, all linked to human infections. Thus, while the samples proved the market served as an “amplifier” of viral spread, they did not prove the market was the source.

Meanwhile, an analysis published on March 16 in the medical journal *BMJ Global Health*, written by a group of Italian scientists and coauthored by Sergei Pond, cites a growing body of studies indicating that the virus may have been spreading worldwide for weeks, or even months, before the officially recognized start date of December 2019. If true, this would entirely upend the presumption of the market as the genesis of the pandemic.

“There are still a lot of credible questions that have not been answered,” says Pond. And with “no overwhelming evidence in either direction,” he adds, he is “puzzled as to why it’s necessary to push in one direction.” (Responding to written questions, Andersen said, “I have no particular stake in the idea that SARS-CoV-2 came from the market and not from virology research. The science speaks for itself and the evidence is clear.”)

Simon Wain-Hobson has his own hypothesis for what is taking place: The group of scientists pushing the claim of natural origin, he says, “want to show that virology is not responsible [for causing the pandemic]. That is their agenda.”

*Additional research by Rebecca Aydin and Stan Friedman.*

## **More Great Stories From *Vanity Fair***

- Can Ukrainian Freedom Fighters Stand Up to the Russian Military?
- Grimes on Music, Mars, and Her Secret New Baby With Elon Musk
- Trump Is Blowing a Gasket Over His Joke of a Social Media Network
- How the Atlanta Spa Shootings Tell a Story of America
- Inside the Succession Drama at Scholastic
- Trump Is Now Spitballing Ways to Launch More Russian War, Then “Sit Back and Watch”
- The Psychology Behind Putin’s War
- From the Archive: How a Once Faceless Putin Took Control of the World’s Largest Country
- Not a subscriber? Join *Vanity Fair* to receive full access to VF.com and the complete online archive now.

# Get the Hive Newsletter

The freshest-and most essential-updates from Washington, Wall Street, and Silicon Valley.

ENTER YOUR E-MAIL ADDRESS

Your e-mail address

SIGN UP

By signing up you agree to our [User Agreement](#) and [Privacy Policy & Cookie Statement](#).

---

READ MORE

---

VIRAL INFLECTION

## The Lab-Leak Theory: Inside the Fight to Uncover COVID-19's Origins

---

Throughout 2020, the notion that the novel coronavirus leaked from a lab was off-limits. Those who dared to push for transparency say toxic politics and hidden agendas kept us in the dark.

BY KATHERINE EBAN

CORONAVIRUS

## In Major Shift, NIH Admits Funding Risky Virus Research in Wuhan

A spokesman for Dr. Fauci says he has been “entirely truthful,” but a new letter belatedly acknowledging the National Institutes of Health’s support for virus-enhancing research adds more heat to the ongoing debate over whether a lab leak could have sparked the pandemic.

BY KATHERINE EBAN



CORONAVIRUS

## “That’s Their Problem”: How Jared Kushner Let the Markets Decide America’s COVID-19 Fate

---

First-person accounts of a tense meeting at the White House in late March suggest that President Trump’s son-in-law resisted taking federal action to alleviate shortages and help Democratic-led New York. Instead, he enlisted a former roommate to lead a Consultant State to take on the Deep State, with results ranging from the Eastman Kodak fiasco to a mysterious deal to send ventilators to Russia.

BY KATHERINE EBAN





INVESTIGATION

# “This Shouldn’t Happen”: Inside the Virus-Hunting Nonprofit at the Center of the Lab-Leak Controversy

Chasing scientific renown, grant dollars, and approval from Dr. Anthony Fauci, Peter Daszak transformed the environmental nonprofit EcoHealth Alliance into a government-funded sponsor of risky, cutting-edge virus research in both the U.S. and Wuhan, China. Drawing on more than 100,000 leaked documents, a *NYT* investigation shows how an organization dedicated to preventing the next pandemic found itself suspected of helping start one.

BY KATHERINE EBAN

MAY 19, 2022



**O**n June 18, 2021, an evolutionary biologist named Jesse D. Bloom sent the draft of an unpublished scientific paper he'd written to Dr. Anthony Fauci, the chief medical adviser to the president of the United States. A bespectacled, boyish-looking 43-year-old often clad in short-sleeved checkered shirts, Bloom specializes in the study of how viruses evolve. "He is the most ethical scientist I know," said Sergei Pond, a fellow evolutionary biologist. "He wants to dig deep and discover the truth."

The paper Bloom had written—known as a preprint, because it had yet to be peer-reviewed or published—contained sensitive revelations about the National Institutes of Health, the federal agency that oversees biomedical research. In the interests of transparency, he wanted Fauci, who helms an NIH subagency, the National Institute of Allergy and Infectious Diseases (NIAID), to see it ahead of time. Under ordinary circumstances, the preprint might have sparked a respectful exchange of views. But this was no ordinary preprint, and no ordinary moment.

More than a year into the pandemic, the genesis of SARS-CoV-2, the virus that causes COVID-19, was still a mystery. Most scientists believed that it had made the leap from bats to humans naturally, via an intermediary species, most likely at a market in Wuhan, China, where live wild animals were slaughtered and sold. But a growing contingent were asking if it could have originated inside a nearby laboratory that is known to have conducted risky coronavirus research funded in part by the United States. As speculation, sober and otherwise, swirled, the NIH was being bombarded by Freedom of Information Act (FOIA) lawsuits. Fauci himself needed a security detail, owing to death threats from conspiracy theorists who believed he was covering up some dark secret.

Bloom's paper was the product of detective work he'd undertaken after noticing that a number of early SARS-CoV-2 genomic sequences mentioned in a published paper from China had somehow vanished without a trace. The sequences, which map the nucleotides that give a virus its unique genetic identity, are key to tracking when the virus emerged and how it might have evolved. In Bloom's view, their disappearance raised the possibility that the Chinese government might be trying to hide evidence about the pandemic's early spread. Piecing together clues, Bloom established that the NIH itself had deleted the sequences from its own archive at the request of researchers in Wuhan. Now, he was hoping Fauci and his boss, NIH director Francis Collins, could help him identify other deleted sequences that might shed light on the mystery.

Bloom had submitted the paper to a preprint server, a public repository of scientific papers awaiting peer review, on the same day that he'd sent a copy to Fauci and Collins. It now existed in a kind of twilight zone: not published, and not yet public, but almost certain to appear online soon.

Collins immediately organized a Zoom meeting for Sunday, June 20. He invited two outside scientists, evolutionary biologist Kristian Andersen and virologist Robert Garry, and allowed Bloom to do the same. Bloom chose Pond and Rasmus Nielsen, a genetic biologist. That it was shaping up like an old-fashioned duel with seconds in attendance did not cross Bloom's mind at the time. But six months after that meeting, he remained so troubled by what transpired that he wrote a detailed account, which *Vanity Fair* obtained.

**Flash Sale Ending Soon**  
**Get 1 year for \$29.99 \$8 + a free tote.**  
**Join now▶**

After Bloom described his research, the Zoom meeting became “extremely contentious,” he wrote. Andersen leapt in, saying he found the preprint “deeply troubling.” If the Chinese scientists wanted to delete their sequences from the database, which NIH policy entitled them to do, it was unethical for Bloom to analyze them further, he claimed. And there was nothing unusual about the early genomic sequences in Wuhan.

Instantly, Nielsen and Andersen were “yelling at each other,” Bloom wrote, with Nielsen insisting that the early Wuhan sequences were “extremely puzzling and unusual.”

Andersen—who'd had some of his emails with Fauci from early in the pandemic publicly released through FOIA requests—leveled a third objection. Andersen, Bloom wrote, “needed security outside his house, and my pre-print would fuel conspiratorial notions that China was hiding data and thereby lead to more criticism of scientists such as himself.”

Fauci then weighed in, objecting to the preprint's description of Chinese scientists “surreptitiously” deleting the sequences. The word was loaded, said Fauci, and the reason they'd asked for the deletions was unknown.

That's when Andersen made a suggestion that surprised Bloom. He said he was a screener at the preprint server, which gave him access to papers that weren't yet public. He then offered to either entirely delete the preprint or revise it “in a way that would leave no record that this had been done.” Bloom refused, saying that he doubted either option was appropriate, “given the contentious nature of the meeting.”

At that point, both Fauci and Collins distanced themselves from Andersen's offer, with Fauci saying, as Bloom recalled it, “Just for the record, I want to be clear that I never suggested you delete or revise the pre-print.” They seemed to know that Andersen had gone too far.

Both Andersen and Garry denied that anyone in the meeting suggested deleting or revising the paper. Andersen said Bloom's account was "false." Garry dismissed it as "nonsense." Sergei Pond, however, confirmed Bloom's account as accurate, after having it read aloud to him. "I don't remember the exact phrasing—I didn't take any notes—but from what you described, that sounds accurate. I definitely felt bad for poor Jesse." He added that the "charged-up" atmosphere struck him as "inappropriate for a scientific meeting." A spokesperson for Fauci declined to comment.

Six months after his contentious meeting with Fauci and other top scientists, on June 20, 2021, Jesse Bloom made a written record of his recollections. *Vanity Fair* later obtained the document. [Click here to see and download the full document.](#)

**T**he wagon-circling on that Zoom call reflected a siege mentality at the NIH whose cause was much larger than Bloom and the missing sequences. It couldn't be made to disappear with creative editing or deletion. And it all began with a once-obscure science nonprofit in Manhattan that had become the conduit for federal grant money to a Wuhan research laboratory.

In 2014, Fauci's agency had issued a \$3.7 million grant to EcoHealth Alliance, a nongovernmental organization dedicated to predicting and helping to prevent the next pandemic by identifying viruses that could leap from wildlife to humans. The grant, titled Understanding the Risk of Bat Coronavirus Emergence, proposed to screen wild and captive bats in China, analyze sequences in the laboratory to gauge the risk of bat viruses infecting humans, and build predictive models to examine future risk. The Wuhan Institute of Virology (WIV) was a key collaborator to whom EcoHealth Alliance gave almost \$600,000 in sub-awards. But the work there had been controversial enough that the NIH suspended the grant in July 2020.

As it happened, EcoHealth Alliance failed to predict the COVID-19 pandemic—even though it erupted into public view at the Huanan Seafood Wholesale Market, a short drive from the WIV itself. In the ensuing months, every move of EcoHealth Alliance, and its voluble president Peter Daszak, came under scrutiny by a small army of scientific sleuths and assorted journalists. What, they wanted to know, had really gone on at the WIV? Why had Daszak been so cagey about the work his organization had been funding there? And were Fauci and other officials trying to direct attention away from research that the U.S. had been, at least indirectly, financing?

The dispute over COVID-19's origins has become increasingly acrimonious, with warring camps of scientists trading personal insults on Twitter feeds. Natural-origin proponents argue that the virus, like so many before it, emerged from the well-known phenomenon of natural spillover, jumping from a bat host to an intermediate species before going on to infect humans. Those suspecting a lab-related incident point to an array of possible scenarios, from inadvertent exposure of a scientist during field research to the accidental release of a natural or manipulated strain during laboratory work. The lack of concrete evidence supporting either theory has only increased the rancor. "Everyone is looking for a smoking gun that would render any reasonable doubt impossible," says Amir Attaran, a biologist and lawyer at the University of Ottawa. Without cooperation from the Chinese government, that may be impossible.

In 2018, Daszak had appeared on Chinese state-run TV and said, "The work we do with Chinese collaborators is published jointly in international journals and the sequence data is uploaded onto the internet free for everyone to read, very open, very transparent, and very collaborative." He added, "Science is naturally transparent and open.... You do something, you discover something, you want to tell the world about it. That's the nature of scientists."

But as COVID-19 rampaged across the globe, the Chinese government's commitment to transparency turned out to be limited. It has refused to share raw data from early patient cases, or participate in any further international efforts to investigate the virus's origin. And in September 2019, three months before the officially recognized start of the pandemic, the Wuhan Institute of Virology took down its database of some 22,000 virus samples and sequences, refusing to restore it despite international requests.

As for transparency-minded scientists in the U.S., Daszak early on set about covertly organizing a letter in the *Lancet* medical journal that sought to present the lab-leak hypothesis as a groundless and destructive conspiracy theory. And Fauci and a small group of scientists, including Andersen and Garry, worked to enshrine the natural-origin theory during confidential discussions in early February 2020, even though several of them privately expressed that they felt a lab-related incident was likelier. Just days before those discussions began, *Vanity Fair* has learned, Dr. Robert Redfield, a virologist and the director of the Centers for Disease Control and Prevention (CDC), had urged Fauci privately to vigorously investigate both the lab and natural hypotheses. He was then excluded from the ensuing discussions—learning only later that they'd even occurred. "Their goal was to have a single narrative," Redfield told *Vanity Fair*.

Why top scientists linked arms to tamp down public speculation about a lab leak—even when their emails, revealed via FOIA requests and congressional review, suggest they held similar concerns—remains unclear. Was it simply because their views shifted in favor of a natural origin? Could it have been to protect science from the ravings of conspiracy theorists? Or to protect against a revelation that could prove fatal to certain risky research that they deem

indispensable? Or to protect vast streams of grant money from political interference or government regulation?

The effort to close the debate in favor of the natural-origin hypothesis continues today. In February, *The New York Times* gave front-page treatment to a set of preprints—written by Michael Worobey at the University of Arizona, Kristian Andersen at Scripps Research Institute, and 16 coauthors, including Garry—claiming that a new analysis of public data from the Huanan market in Wuhan provided “dispositive evidence” that the virus first leapt to humans from animals sold there. But a number of top scientists, Bloom among them, questioned that assertion, saying the preprints, while worthy, relied on incomplete data and found no infected animal.

“I don’t think they offer proof. They provide evidence that more strongly supports the link to the wild animal market than to the WIV, and that’s the way I would have phrased it,” says W. Ian Lipkin, an epidemiologist at Columbia University who favors the natural-origin theory.

“Some scientists seem almost hell-bent on naming the Huanan market as the site of the origin of the pandemic; and some members of the media seem more than happy to embrace these conclusions without careful examination,” said Stanford microbiologist David Relman. “This issue is far too important to be decided in the public domain by unreviewed studies, incomplete and unconfirmed data, and unsubstantiated proclamations.”

Perhaps more than anyone, Peter Daszak—a Western scientist immersed in Chinese coronavirus research at the Wuhan Institute of Virology—was uniquely positioned to help the world crack open the origin mystery, not least by sharing what he knew. But last year, Dr. Jeffrey Sachs, the Columbia University economist who oversees the *Lancet*’s COVID-19 commission, dismissed Daszak from the helm of a task force investigating the virus’s genesis, after he flatly refused to share progress reports from his contested research grant. (In written responses to detailed questions, Daszak said he was “simply following NIH guidance” when he declined Sachs’s request, because the agency was withholding the reports in question “until they had adjudicated a FOIA request.” The reports are now publicly available, he said.)

“[Daszak] and NIH have acted badly,” Sachs told *Vanity Fair*. “There has been a lack of transparency...and there is a lot more to know and that can be known.” He said that the NIH should support an “independent scientific investigation” to examine the “possible role” in the pandemic of the NIH, EcoHealth Alliance, the Wuhan Institute of Virology, and a partner laboratory at the University of North Carolina. “Both hypotheses are still very much with us,” he said, and “need to be investigated seriously and scientifically.” (“We are also on record as welcoming independent scientific investigation into the origins of the COVID-19 pandemic,” Daszak told *Vanity Fair*.)

This story is based on more than 100,000 internal EcoHealth Alliance documents obtained by *Vanity Fair*, as well as interviews with five former staff members and 33 other sources. The documents, most of which predate the pandemic, span a number of years and include budgets, staff and board meeting minutes, and internal emails and reports. While the documents do not tell us where COVID-19 came from, they shed light on the world in which EcoHealth Alliance has operated: one of murky grant agreements, flimsy oversight, and the pursuit of government funds for scientific advancement, in part by pitching research of steeply escalating risk.

**T**he story of how Daszak's grant entangled Fauci in the specter of Wuhan coronavirus research began years earlier, at a stately Beaux Arts social club in Washington, D.C. For more than a decade, EcoHealth Alliance hosted a series of cocktail parties at the Cosmos Club near DuPont Circle to discuss the prevention of viral outbreaks. There, expert biologists, virologists, and journalists mingled with the true guests of honor: federal government bureaucrats who were in the position to steer grants.

On invitations, EcoHealth Alliance described the events as “educational.” Inside the nonprofit, however, officials called them “cultivation events.” The return on investment was excellent: For about \$8,000 in Brie and Chardonnay per event, they got to network with prospective federal funders. As the organization's 2018 strategic plan spelled out, “Given our strength in federal funding, we enhanced our cultivation events at the Cosmos Club in Washington DC, which now regularly attract 75-150 people at high levels in govt agencies, NGOs and the private sector.” (“These kinds of events are common among many nongovernmental organizations and nonprofits, which depend upon both public and private donors for support,” Daszak told *Vanity Fair*.)

Of all those high-level people, almost no one ranked as high as Fauci, a scientific kingmaker who dispensed billions in grant money each year—and Daszak was determined to share a podium with him. The idea was admittedly a reach. Though he'd met with Fauci and received funding from his agency, Daszak was relatively obscure. But he had cultivated back-channel access to the minders who guarded Fauci's calendar.

On September 9, 2013, Daszak emailed Fauci's senior adviser David Morens to see if the sought-after NIAID chief would be available as a panel speaker. Morens emailed back, recommending that Daszak “write Tony directly, thanking him for meeting with you all recently and then inviting him to be a member of this Cosmos Club discussion. That way, it is personal and doesn't look ‘cooked’ by us.”

Though Fauci declined that invitation and several others, Daszak kept trying. In February 2016, Morens passed along a valuable tip: Fauci “normally says no to almost everything like this.



Unless ABC, NBC, CBS, and Fox are all there with cameras running. If he were asked to give THE main talk or the only talk that might increase the chances.”

The gambit worked. Fauci signed on to give a presentation on the Zika virus at the Cosmos Club on March 30, and the RSVPs flowed in. The guests came from an array of deep-pocketed federal agencies: the Department of Homeland Security, the U.S. Agency for International Development, the Pentagon, even NASA. As Daszak would declare at a board meeting on December 15, the “Washington, DC cultivation events have been a great way to increase our visibility to federal funders,” according to meeting minutes. A month earlier, Donald Trump had been elected president. One board member at the meeting asked what his incoming administration might mean for a conservation nonprofit dependent on federal grants. Daszak offered breezy reassurance: The organization’s “apolitical mission” would help it adapt.

Little did he know that, in the era of Trump and COVID-19, science itself would become the ultimate political battleground.

EcoHealth Alliance's D.C. "cultivation events," whose guest speakers would include Dr. Anthony Fauci, are said in board meeting minutes to improve "visibility" to federal funders. [Click here to see and download the full document.](#)

f a shared podium with Fauci proved that Daszak had become a true player among virus hunters, it also underscored just how far he had come. For years, Peter Daszak sat at the helm of a struggling nonprofit with a mission to save manatees, promote responsible pet ownership, and celebrate threatened species. The organization, which operated under the name Wildlife Trust until 2010, was constantly on the hunt for ways to close its budget shortfalls. One year, it proposed to honor at its annual benefit a mining company operating in Liberia that was paying it to assess the risks of Ebola virus. Another idea was to seek donations from palm-oil millionaires leveling rainforests who might be interested in “cleaning up” their image.

Balding and usually clad in hiking gear, Daszak was one part salesman, one part visionary. He saw clearly that human incursions into the natural world could lead to the emergence of animal pathogens, with bats a particularly potent reservoir. Daszak was “making a bet that bats were harboring deadly viruses,” said Dr. Matthew McCarthy, an associate professor of medicine at Weill Cornell Medical Center in New York. In 2004, as a 23-year-old Harvard medical student, McCarthy followed Daszak to Cameroon to trap bats. “I left my family, my friends,” he said. “It was a very powerful thing for people like me, going into the most remote parts of the world. I was taken by him, hook, line, and sinker.”

The bioterror attacks of 2001, in which letters dusted with anthrax spores were sent through the U.S. mail, coupled with the first SARS coronavirus outbreak in China the following year, would bring money for the study of lethal natural pathogens pouring into federal agencies. In 2003, the NIAID got an eye-popping \$1.7 billion for research to defend against bioterrorism.

Daszak’s office on Manhattan’s Far West Side didn’t have a laboratory. The closest bat colonies were in Central Park. But he cultivated an affiliation with Shi Zhengli, a Chinese scientist who would rise to become the director of the Wuhan Institute of Virology’s Center for Emerging Infectious Diseases. Slight and sophisticated with an international education, Shi became known in China as “bat woman” for her fearless exploration of their habitats. Daszak’s alliance with her would open China’s bat caves to him.

In 2005, after conducting field research in four locations in China, Daszak and Shi coauthored their first paper together, which established that horseshoe bats were a likely reservoir for SARS-like coronaviruses. They would go on to collaborate on 17 papers. In 2013, they reported their discovery that a SARS-like bat coronavirus, which Shi had been the first to successfully isolate in a lab, might be able to infect human cells without first jumping to an intermediate animal.

“[Peter] respected her,” said the former EcoHealth Alliance staffer. “In the view of everyone, they were doing great work for the world.” Their partnership gave Daszak an almost proprietary sense of the bat caves in Yunnan province, which he would later refer to in a grant proposal as “our field test sites.”

As Daszak's staff and Shi's graduate students intermingled, traveling between Wuhan and Manhattan, the exchange flourished. When Shi visited New York, the EcoHealth staff selected a restaurant for a celebratory dinner with great care. "Zhengli is not one to stand on formality; she makes dumplings by hand with her students in the lab!!" Daszak's chief of staff wrote to another employee. "She got her PhD in France, loves red wine, and likes good food above formality."

By 2009, bats had turned into big money. That September, USAID awarded a \$75 million grant called PREDICT to four organizations, including Daszak's. It was "the most comprehensive zoonotic virus surveillance project in the world," USAID stated, and its purpose was to identify and predict viral emergence, in part by sampling and testing bats and other wildlife in remote locations.

The \$18 million over five years awarded to what was then Wildlife Trust was a "game-changer," Daszak told his staff in an ecstatic email sharing the news. "I want to take this opportunity (despite 7 hours of drinking champagne – literally!) to thank all of you for your support."

The money transformed the ragged nonprofit. It increased its budget by half, ending a yearslong operating loss; began a long-deferred rebranding, which led to the new name EcoHealth Alliance; and spruced up its headquarters, even fixing its chronically broken air conditioner. Over the course of the grant, it allocated \$1.1 million to the Wuhan Institute of Virology, USAID recently acknowledged in a letter to Congress.

**W**hen Dr. Maureen Miller, an infectious disease epidemiologist, arrived at EcoHealth Alliance in 2014, she landed in an environment that she found to be toxic and secretive. Closed-door meetings were the norm. The senior leadership constituted an unwelcoming "old boys network." She soon came to believe that she was hired "because they needed a senior-level woman," she said, adding, "I was excluded from pretty much everything."

She came aboard shortly before the organization's PREDICT grant was renewed for five more years. It was also the year the NIH approved Understanding the Risk of Bat Coronavirus Emergence, the \$3.7 million grant that would come back to haunt Fauci. Miller said she was "lured by the idea of being able to create a pandemic-threats warning system."

Miller got to work creating a surveillance strategy to detect zoonotic virus spillover. Chinese villagers living near bat caves in Southern Yunnan province would have their blood tested for antibodies to a SARS-like coronavirus, then answer questionnaires to determine if certain behaviors had led them to be exposed. It was a "biological and behavioral warning system," Miller explained.

Over the next two years, Miller saw Daszak only a handful of times. But she worked closely with Shi Zhengli, who developed the test to screen the villagers' blood. In that time, Miller noted, "I never got a result from [Shi] via phone. I had to show up in China to learn anything from her." From that, Miller gleaned that, while Shi was a "world-class scientist, she respects the Chinese system." In short, she followed the Chinese government's rules. (Shi Zhengli did not respond to written questions for this article.)

Miller left EcoHealth Alliance in November 2016, never knowing what became of the strategy she'd developed. But in the fall of 2017, Shi alerted Miller's former assistant to the fact that Daszak was about to get credit for her work in an upcoming publication. "Shi went out of her way to ensure I would be included," Miller said. The final version of a letter, published in January 2018 in the Wuhan Institute of Virology's journal, *Virologica Sinica*, included Miller's name. Six out of 218 villagers had tested positive for antibodies, suggesting that the strategy was a successful way to gauge potential spillover.

But the experience left Miller with a dark impression of Daszak: "He is so single-minded that he wants to be the one who makes the discovery, without having to share."

Daszak said Miller has been credited as a coauthor on at least eight papers stemming from her work at EcoHealth Alliance, "a testimony to the equity, fairness, and openness of our publication and authorship practices." He added that the nonprofit's staff is "diverse and culturally sensitive" and has been "majority female for 20 years."

**D**aszak's \$3.7 million NIH grant first set off alarm bells in early May 2016, as it entered its third year. The NIH requires annual progress reports, but Daszak's year-two report was late and the agency threatened to withhold funds until he filed it.

The report he finally did submit worried the agency's grant specialists. It stated that scientists planned to create an infectious clone of Middle East Respiratory Syndrome (MERS), a novel coronavirus found in dromedaries that had emerged in Saudi Arabia in 2012 and killed 35% of the humans it infected. The report also made clear that the NIH grant had already been used to construct two chimeric coronaviruses similar to the one that caused Severe Acute Respiratory Syndrome (SARS), which emerged in 2002 and went on to cause at least 774 deaths worldwide. (A chimeric virus is one that combines fragments of different viruses.) These revelations prompted the NIH's grant specialists to ask a critical question: Should the work be subject to a federal moratorium on what was called gain-of-function research?

With that, Daszak's grant got tangled in a yearslong debate that had divided the virology community. In 2011, two scientists separately announced that they had genetically altered

Highly Pathogenic Asian Avian Influenza A (H5N1), the bird flu virus that has killed at least 456 people since 2003. The scientists gave the virus new functions—enabling it to spread efficiently among ferrets, which are genetically closer to humans than mice—as a way to gauge its risks to people. Both studies had received NIH funding.

The scientific community erupted in conflict over what became known as gain-of-function research. Proponents claimed it could help prevent pandemics by highlighting potential threats. Critics argued that creating pathogens that didn't exist in nature ran the risk of unleashing them. As the dispute raged, Fauci worked to strike a middle ground, but ultimately supported the research, arguing in a coauthored *Washington Post* op-ed that “important information and insights can come from generating a potentially dangerous virus in the laboratory.”

In October 2014, the Obama administration imposed a moratorium on new federal funding for research that could make influenza, MERS, or SARS viruses more virulent or transmissible, while a review took place. But the moratorium, as written, left loopholes, which allowed Daszak to try to save the research. On June 8, 2016, he wrote to the NIH's grant specialists that the SARS-like chimeras from the completed experiment were exempt from the moratorium, because the strains used had not previously been known to infect humans. He also pointed to a 2015 research paper in which scientists had infected humanized mice with the same strains, and found that they were less lethal than the original SARS virus.

But the 2015 research paper he cited was not particularly reassuring. In it, Shi Zhengli and a preeminent coronavirus researcher at the University of North Carolina, Ralph Baric, mixed components of SARS-like viruses from different species, and created a novel chimera that was able to directly infect human cells. (Baric did not respond to written questions seeking comment.)

This gain-of-function experiment, which had begun prior to the moratorium, was so fraught that the authors flagged the dangers themselves, writing, “scientific review panels may deem similar studies...too risky to pursue.” The paper's acknowledgments cited funding from the NIH and from EcoHealth Alliance, through a different grant.

If anything, the MERS study Daszak proposed was even riskier. So he pitched a compromise to the NIH: that if any of the recombined strains showed 10 times greater growth than a natural virus, “we will immediately: i) stop all experiments with the mutant, ii) inform our NIAID Program Officer and the UNC [Institutional Biosafety Committee] of these results and iii) participate in decision making trees to decide appropriate paths forward.”

This mention of UNC brought a puzzled response from an NIH program officer, who pointed out that the proposal had said the research would be performed at the WIV. “Can you clarify where

the work with the chimeric viruses will actually be performed?" the officer wrote. Ten days later, with still no response from Daszak, the program officer emailed him again. On June 27, Daszak responded, buoyant as ever:

---

*"You are correct to identify a mistake in our letter. UNC has no oversight of the chimera work, all of which will be conducted at the Wuhan Institute of Virology.... We will clarify tonight with Prof. Zhengli Shi exactly who will be notified if we see enhanced replication...my understanding is that I will be notified straight away, as [principal investigator], and that I can then notify you at NIAID. Apologies for the error!"*

By July 7, the NIH agreed to Daszak's terms, which relied entirely on mutual transparency: Shi would inform him of any concerning developments involving the lab-constructed viruses, and he would inform the agency. Daszak replied enthusiastically to a program officer, "This is terrific! We are very happy to hear that our Gain of Function research funding pause has been lifted."

Allowing such risky research to go forward at the Wuhan Institute of Virology was "simply crazy, in my opinion," says Jack Nunberg, director of the Montana Biotechnology Center. "Reasons are lack of oversight, lack of regulation, the environment in China," where scientists who publish in prestigious journals get rewarded by the government, creating dangerous incentives. "So that is what really elevates it to the realm of, 'No, this shouldn't happen.'"

A subsequent development seemed to support that view. On January 15, 2021, in the waning days of the Trump administration, the State Department released a fact sheet based on declassified intelligence. It asserted that Chinese military scientists had been collaborating with the WIV's civilian scientists since 2017, if not earlier. That raised the question of whether research there was being repurposed for offensive or military uses. Though Shi and other WIV leaders have previously denied such collaboration occurred, former deputy national security adviser Matthew Pottinger calls those denials "willful lies. If one were to give them the benefit of the doubt, you might go so far as to say they have no choice but to lie, but these are lies nonetheless."

If China's military had been collaborating with WIV scientists, it's unclear if Daszak would have realized it. He had far less visibility into the WIV than he let on, a former EcoHealth Alliance staffer told *Vanity Fair*. The work being done there was "always an enigma," the former staffer said. The nonprofit had hired a U.S.-based Chinese national who helped "interpret for them what was happening inside the WIV.... But we had to take everything at face value. It was more, 'Accept what it is, because of this relationship'" between Shi and Daszak.

"He doesn't know what happened in that lab," said the former staffer. "He cannot know that."

According to Daszak, EcoHealth Alliance “was aware” of the WIV’s research activities related to its NIH grant. He says he had no knowledge of Chinese military involvement there and was never notified of any by the U.S. government.

**B**y 2017, despite massive infusions of grant money, EcoHealth Alliance faced a brewing financial crisis. Ninety-one percent of its funding came from the federal government, and 71% of that came from the PREDICT grant, according to minutes of the organization’s finance committee meeting. The renewed grant, known as PREDICT II, was slated to end in two years. There was no way to know if the grant would be reauthorized for a third time. The looming possibility that it would expire came to be known internally as the “PREDICT cliff.”

How to prevent the organization from tumbling over it consumed meeting after meeting. One possible solution was the Global Virome Project, a nongovernmental initiative being organized by the infectious disease specialist Dennis Carroll, who had established PREDICT while working at USAID. The Global Virome Project was far more ambitious: Its goal was to map every possible virus on earth—an estimated 840,000 of which might infect human beings—as a way to “end the pandemic era.”

The program had a steep projected price tag of \$3.4 billion over 10 years, Daszak explained to board members. But the cost of not knowing and suffering a pandemic was estimated at \$17 trillion over 30 years. Looked at that way, the Global Virome Project was a relative bargain.

But there was another way that EcoHealth Alliance could ward off the \$8 million shortfall it was facing. The Defense Department could serve as a federal life raft in a new ocean of grants. The Defense Advanced Research Projects Agency (DARPA) was seeking proposals for a new program called PREEMPT, which aimed to identify animal pathogens “to preempt their entry into human populations before an outbreak occurs.”

For EcoHealth Alliance, the PREEMPT grant seemed like a slam dunk. For years, Daszak had been developing a method of predictive modeling to identify likely sites of viral spillover around the world and stop pandemics at the source. Some questioned the effectiveness of Daszak’s approach. “In 20 years of using this method, [EcoHealth Alliance] did not predict a single outbreak, epidemic or pandemic,” Maureen Miller told *Vanity Fair*. But David Morens, senior adviser to the NIAID director, said that Daszak became one of the “key players” in understanding that “emerging diseases came from animals, the animals had their own geographic ranges, and if you knew where the animals were and what diseases they carried, you could predict hot spots.”

EcoHealth Alliance also doubled down on another key selling point: Its unique on-the-ground connections in China would effectively give the U.S. government a foothold in foreign



laboratories. As Daszak had told his staff at a meeting some years earlier, one Defense Department subagency wanted “information on what is going on in countries in which they cannot access (China, Brazil, Indonesia, India).”

With the PREDICT cliff and the DARPA deadline coming ever closer, Daszak struck an upbeat note with his board, pointing out that the organization had a strong track record of winning federal grants. “This was the golden ticket,” a former staffer familiar with the DARPA grant application said. “The message was always, ‘We are going to do cool and cutting-edge science. DARPA is the right agency to fund this.’”

**L**ast September, EcoHealth Alliance’s grant proposal to DARPA was leaked to DRASTIC, a loosely affiliated global group of sleuths—ranging from professional scientists to amateur data enthusiasts—dedicated to investigating the origins of COVID-19. From the 75-page proposal, a striking detail stood out: a plan to examine SARS-like bat coronaviruses for furin cleavage sites and possibly insert new ones that would enable them to infect human cells.

A furin cleavage site is a spot in the surface protein of a virus that can boost its entry into human cells. SARS-CoV-2, which emerged more than a year after the DARPA grant was submitted, is notable among SARS-like coronaviruses for having a unique furin cleavage site. This anomaly has led some scientists to consider whether the virus could have emerged from laboratory work gone awry.

Documents obtained by *Vanity Fair* shed new light on the chaotic process surrounding the DARPA proposal, which was cocreated with colleagues including Shi Zhengli at the WIV and Ralph Baric at the University of North Carolina at Chapel Hill. As the March deadline approached, the grant’s collaborators worked 24/7, with versions pouring in from around the world. “Those documents were being written by many, many people,” one former employee recalled.

The grant application proposed to collect bat samples from caves in Yunnan Province, transport them to the Wuhan Institute of Virology, extract and manipulate the viruses they contain, and use them to infect mice with humanized lungs. It would then map high-risk areas for bats harboring dangerous pathogens and treat test caves with substances to reduce the amount of virus they were shedding.

It was a long way from saving manatees from motorboats.

By almost any definition, this was gain-of-function research. The federal moratorium had been lifted in January 2017 and replaced with a review system called the HHS P3CO Framework (for

Potential Pandemic Pathogen Care and Oversight). This required a safety review by the agency funding the research.

EcoHealth Alliance's DARPA proposal asserted that its research was exempt from the P3CO framework. It also emphasized the extensive experience of the team it would assemble. But at a staff meeting on March 29, Daszak expressed dismay at the slapdash and amateur nature of the DARPA submission. It was a "major failure on all accounts," he noted, enumerating a cascade of mistakes: The application was late, sent in "30 minutes after deadline." There were errors uploading documents, comment boxes that remained on the pages, a question of who was in charge. What was needed, he exhorted his staff, was a "change in culture" as "part of [a] mentality [sic] to get money," according to the meeting minutes.

EcoHealth Alliance's controversial rejected DARPA grant proposal is described as a "major failure" in staff meeting minutes. [Click here](#) to see and download the document.

Inside DARPA, the grant application was met with immediate skepticism. The contract was “never awarded because of the horrific lack of common sense” it reflected, said a former DARPA official who was there at the time. EcoHealth Alliance was viewed as a “ragtag group” and a “middle guy,” a backseat collaborator willing to get on an Air China jet, eat terrible food, and stay in bad hotels, said the former official.

Likewise, the WIV was also viewed as subpar, especially when compared with the Harbin Veterinary Research Institute, which operated China’s only other high-containment laboratory with the highest biosafety protocol: BSL-4. Harbin was China’s Harvard, said the former DARPA official. The WIV was more like a safety school. EcoHealth Alliance had “bolted on” a serious scientist, Ralph Baric, and “podged” the proposal together. Having the nonprofit serve as the prime contractor for a global project with national security risks was like “having your rental car agency trying to run an armada,” said the former DARPA official.

Though two of three DARPA reviewers deemed it “selectable,” the third, a program manager in the Biological Technologies Office, recommended against funding it. He wrote that the application did not adequately mention or assess the gain-of-function risk or the possibility that the proposed work could constitute dual-use research of concern (DURC), the technical term for science that can be repurposed to cause harm or endanger security.

The DARPA proposal was “basically a road map to a SARS-CoV-2-like virus,” says virologist Simon Wain-Hobson, who is among the scientists calling for a fuller investigation of COVID-19’s origins. If the research had the blessing of a top coronavirus scientist like Baric, then it is possible the WIV would have wanted to copy what it viewed as cutting-edge science, he said. “That doesn’t mean they did it. But it means it’s legitimate to ask the question.”

According to Daszak, no one at DARPA expressed any concerns about the proposed research to EcoHealth Alliance. On the contrary, he said, “DARPA told us that ‘we had a strong proposal’ and ‘wished DARPA had greater funding for the PREEMPT program.’” He added, “the research was never done by EHA or, to my knowledge, any of the collaborating partners on that proposal.”

**B**y late December 2019, cases of what would soon be identified as SARS-CoV-2 began emerging around the Huanan Seafood Wholesale Market in the Jiangnan district of Wuhan, roughly eight miles from the Wuhan Institute of Virology.

Daszak seemed poised to play a leading role in the emerging crisis. On January 2, 2020, he tweeted: “The GOOD news!! is that leading scientists from the US, China and many other countries are working together to actively block the ability of these viruses to spillover, and to rapidly detect them if they do.” He continued, “This includes active collaboration with China

CDC, Wuhan Inst. Virology, @DukeNUS, @Baric\_Lab, and a diverse array of Provincial CDCs, universities and labs across S. and Central China.”

On January 30, Daszak went on CGTN America, the U.S. outpost for Chinese state television, and said two things that proved to be spectacularly wrong. “I’m very optimistic...that this outbreak will begin to slow down,” he said. “We’re seeing a small amount of human-to-human transmission in other countries, but it’s not uncontrollable.” He went on to conclude that the Chinese government was taking all necessary steps “to be open and transparent, and work with WHO, and talk to scientists from around the world, and where necessary, bring them in to help. They’re doing that. It’s exactly what needs to happen.”

In fact, the opposite was true. The virus was spreading uncontrollably and the Chinese government was busy crushing anyone who spoke out: It ordered laboratory samples destroyed, punished doctors who raised alarms, and claimed the right to review any scientific research about COVID-19 ahead of publication, a restriction that remains in place today.

At the highest levels of the U.S. government, alarm was growing over the question of where the virus had originated and whether research performed at the WIV, and funded in part by U.S. taxpayers, had played some role in its emergence.

To Dr. Robert Redfield, the director of the CDC at the time, it seemed not only possible but likely that the virus had originated in a lab. “I personally felt it wasn’t biologically plausible that [SARS CoV-2] went from bats to humans through an [intermediate] animal and became one of the most infectious viruses to humans,” he told *Vanity Fair*. Neither the 2002 SARS virus nor the 2012 MERS virus had transmitted with such devastating efficiency from one person to another.

What had changed? The difference, Redfield believed, was the gain-of-function research that Shi and Baric had published in 2015, and that EcoHealth Alliance had helped to fund. They had established that it was possible to alter a SARS-like bat coronavirus so that it would infect human cells via a protein called the ACE2 receptor. Although their experiments had taken place in Baric’s well-secured laboratory in Chapel Hill, North Carolina, who was to say that the WIV had not continued the research on its own?

In mid-January of 2020, *Vanity Fair* can reveal, Redfield expressed his concerns in separate phone conversations with three scientific leaders: Fauci; Jeremy Farrar, the director of the U.K.’s Wellcome Trust; and Tedros Adhanom Ghebreyesus, director general of the World Health Organization (WHO). Redfield’s message, he says, was simple: “We had to take the lab-leak hypothesis with extreme seriousness.”

It is not clear whether Redfield’s concerns are what sparked Fauci’s own. But on Saturday night, February 1, at 12:30 a.m., Fauci emailed the NIAID’s principal deputy director, Hugh

Auchincloss, under the subject line “IMPORTANT.” He attached the 2015 paper by Baric and Shi and wrote, “Hugh: It is essential that we speak this AM. Keep your cell phone on.” He instructed Auchincloss to read the attached paper and added, “You will have tasks today that must be done.”

February 1 proved to be a critical day. With the death count in China passing 300 and cases popping up in more than a dozen countries, Farrar convened a group of 11 top scientists across five time zones. That morning, he asked Fauci to join. “My preference is to keep this group really tight,” Farrar wrote. “Obviously ask everyone to treat in total confidence.” Fauci, Francis Collins, Kristian Andersen, and Robert Garry all joined the call. No one invited Redfield, or even told him it was happening.

In the conference call and emails that followed over the next four days, the scientists parsed the peculiarities of SARS-CoV-2’s genomic sequence, paying special attention to the furin cleavage site.

Dr. Michael Farzan, an immunologist, emailed the group, writing that the anomaly could result from sustained interaction between a chimeric virus and human tissue in a laboratory that lacked appropriate biocontainment protocols, “accidentally creating a virus that would be primed for rapid transmission between humans.” He leaned toward the lab-origin hypothesis, saying, “I think it becomes a question of...whether you believe in this series of coincidences, what you know of the lab in Wuhan, how much could be in nature—accidental release or natural event? I am 70:30 or 60:40.”

He was not alone. Garry wrote of the “stunning” composition of the furin cleavage site: “I really can’t think of a plausible natural scenario where you get from the bat virus or one very similar to it to [SARS-CoV-2] where you insert exactly 4 amino acids 12 nucleotide[s] that all have to be added at the exact same time to gain this function.... I just can’t figure out how this gets accomplished in nature.”

The previous evening, Andersen had emailed Fauci, saying that he and scientists including Garry, Farzan, and the Australian virologist Edward Holmes all found the genetic sequence “inconsistent with expectations from evolutionary theory.”

But within three days, four of the scientists on the call, including Andersen, Garry, and Holmes, had shared the draft of a letter arguing the opposite. Farrar shared a copy with Fauci, who offered feedback ahead of its publication on March 17 in *Nature Medicine*. The letter, *The Proximal Origin of SARS-CoV-2*, analyzed the genomic sequence and made a seemingly unequivocal statement: “we do not believe that any type of laboratory-based scenario is plausible.”

How they arrived at such certainty within four days remains unclear. In his book *Spike: The Virus vs. The People—the Inside Story*, Farrar cited “the addition of important new information, endless analyses, intense discussions and many sleepless nights.” But even as they circulated the draft on February 4, qualms remained. Farrar wrote to Collins and Fauci that, while Holmes now argued against an engineered virus, he was still “60-40 lab.”

A Wellcome spokesman told *Vanity Fair*, “Dr. Farrar is in regular conversation with and regularly convenes many other expert scientists.” He added, “Dr. Farrar’s view is that there was at no stage any political influence or interference during these conversations, or in the research carried out.” Garry said that it was “frankly tiresome to explain for the umpteenth time that that was one email cherry-picked among dozens, even hundreds, in part of an ongoing scientific discussion.”

Though he wasn’t part of those conversations, the epidemiologist W. Ian Lipkin told *Vanity Fair*, “I have known Fauci for 30 years. Fauci is not interested in anything but the truth. Anyone that says anything otherwise doesn’t know him.”

Lipkin was added as a fifth author on the Proximal Origin letter. Ahead of publication, he told his coauthors he was concerned that gain-of-function research on coronaviruses was being performed in laboratories with insufficient safeguards. The Proximal Origin letter addresses that issue, but dismisses a possible accident as the source of SARS-CoV-2. Lipkin was not invited to participate in future publications with the group, such as the preprints by Andersen and Worobey that made it onto the front page of *The New York Times* in February. “I can speculate on why I’ve not been asked to join various publications. However, I don’t know why I’ve not been asked,” he said.

While Andersen and the others were fine-tuning the Proximal Origin letter, Daszak was quietly working to bury speculation of a lab leak. On February 19, in a letter published in the influential medical journal *The Lancet*, he joined 26 scientists in asserting, “We stand together to strongly condemn conspiracy theories suggesting that COVID-19 does not have a natural origin.” Nine months later, emails released by a Freedom of Information group showed that Daszak had orchestrated the *Lancet* statement with the intention of concealing his role and creating the impression of scientific unanimity.

Under the subject line, “No need for you to sign the ‘Statement’ Ralph!!,” he wrote to Baric and another scientist: “you, me and him should not sign this statement, so it has some distance from us and therefore doesn’t work in a counterproductive way.” Daszak added, “We’ll then put it out in a way that doesn’t link it back to our collaboration so we maximize an independent voice.”

Baric agreed, writing back, “Otherwise it looks self-serving and we lose impact.”

The *Lancet* statement ended with a declaration of objectivity: “We declare no competing interests.” Among its signatories were Jeremy Farrar and one other participant in the confidential huddle with Fauci.

Reading the *Lancet* letter, with Farrar’s name attached to it, Redfield had a dawning realization. He concluded there’d been a concerted effort not just to suppress the lab-leak theory but to manufacture the appearance of a scientific consensus in favor of a natural origin. “They made a decision, almost a P.R. decision, that they were going to push one point of view only” and suppress rigorous debate, said Redfield. “They argued they did it in defense of science, but it was antithetical to science.”

A Wellcome spokesperson told *Vanity Fair*, “The letter was a simple statement of solidarity with highly reputable researchers based in China and against non-evidence-based theories. Dr. Farrar does not believe the letter was covertly organized. He had no conflict of interest to declare.”

**A**s the pandemic spread to every corner of the globe, Daszak continued to devote his considerable energies to promoting the idea that science itself had reached consensus: The virus emerged from nature, not a lab. But as one concerning detail after another slipped into public view, the facade of unanimity began to crack, exposing his own work to questions.

During a White House COVID-19 press briefing on April 17, 2020, a reporter for the right-wing television network Newsmax asked President Trump why the NIH would fund a \$3.7 million grant to a high-level lab in China. The details were wrong, and the question seemed queued-up to feed an anti-China political agenda. Trump responded, “We will end that grant very quickly.”

That exchange, in turn, uncorked a question from another reporter to Fauci: Could SARS-CoV-2 have come from a lab? His answer from the White House podium was swift and clear. A recently published analysis from a “group of highly qualified evolutionary virologists” had concluded that the virus was “totally consistent with a jump of a species from an animal to a human.” He was referring to the Proximal Origin letter, drafted by some of the scientists he’d met with confidentially in early February.

The next day, Daszak sent an email of profuse thanks to Fauci for “publicly standing up and stating that the scientific evidence supports a natural origin for COVID-19 from a bat-to-human spillover, not a lab release from the Wuhan Institute of Virology.” Fauci responded, thanking him back.

If Daszak thought that Fauci’s kind words meant his grant was safe, he was mistaken. Six days later, he received a sharply worded letter from a senior NIH official: His bat coronavirus

research grant, which had provided subgrants to the WIV, was being terminated. Amid an uproar and legal threats, the agency reinstated the grant several months later, but suspended its activities. So began a bitter, ongoing battle between Daszak and the NIH over whether he'd complied with the grant's terms. Swaths of this private correspondence have become public since last September, as part of a FOIA lawsuit waged by The Intercept.

Daszak also found himself answering increasingly pointed questions about the WIV's decision to take down its online database of 22,000 genomic sequences in September 2019, prior to the known onset of the pandemic.

Maureen Miller says the human blood samples that were collected in China as part of the surveillance strategy she designed at EcoHealth Alliance could hold clues to COVID-19's provenance. But they went into the WIV and are now out of reach. Why would a database supported by U.S. tax dollars to help prevent and respond to a pandemic be made "inaccessible exactly when it was needed to fulfill its intended purpose?" asks Jamie Metzl, a senior fellow at the Atlantic Council, who was among the first to call for a full investigation of COVID-19's origins.

Presumably, Daszak possessed a great deal of that inaccessible data. He said as much during a March 2021 panel organized by a London-based think tank: "A lot of this work has been conducted with EcoHealth Alliance.... We do basically know what's in those databases." Previously, EcoHealth Alliance had signed a pledge, along with 57 other scientific and medical organizations, to share data promptly in the event of a global public health emergency. And yet, in the face of just such an emergency, Daszak told *Nature* magazine, "We don't think it's fair that we should have to reveal everything we do."

In April 2020, he warned colleagues from other institutions that partnered on the PREDICT grants not to publicly release certain sequences. "All - It's extremely important that we don't have these sequences as part of our PREDICT release to Genbank at this point," he wrote. "As you may have heard, these were part of a grant just terminated by NIH. Having them as part of PREDICT will [bring] very unwelcome attention to" the PREDICT program, grant partners, and USAID.

By October 2021, the NIH had repeatedly demanded that EcoHealth Alliance turn over data related to its grant research with the WIV. Daszak argued that he couldn't share a number of SARS coronavirus sequences because he was waiting for the Chinese government to authorize their release. The explanation seemed to undercut the entire rationale for having the U.S. government help fund a global collaboration on virus emergence.



Daszak said it was “incorrect” to suggest that EcoHealth Alliance had not “readily shared data,” and asserted that all of its relevant coronavirus data from NIH-supported research at the WIV has now been made public. He added that he warned about “unwelcome attention” because he wanted “to avoid [colleagues] being dragged into the political fray unfairly” after the NIH’s decision to terminate EcoHealth Alliance’s grant “unleashed a torrent of unwarranted political attacks.”

**U**S. officials and at least one of Daszak’s former colleagues were stunned when, in November 2020, the WHO announced the names of 11 international experts assigned to a fact-finding mission to China to investigate COVID-19’s origins. China had veto power over the list, and none of the three candidates put forward by the U.S. had made the cut. Instead, Peter Daszak was listed as America’s sole representative.

It’s still unclear how Daszak wound up on the commission. “I didn’t want to go, and I said no initially,” he later told *Science* magazine, before adding, “If you want to get to the bottom of the origins of a coronavirus outbreak in China, the number one person you should be talking to is the person who works on coronaviruses in China, who’s not from China.... So that’s me, unfortunately.”

Daszak told *Vanity Fair*, “WHO reached out to me and asked me to serve on the committee. I initially refused, but...following their persuasive arguments decided that it was my duty as a scientist to support the origins investigation.” A WHO spokesperson would neither confirm nor deny Daszak’s account.

One former EcoHealth staffer thinks it’s obvious who tapped Daszak for the role: “If his name was not among the names floated [by the U.S.], his was the name that the Chinese government chose.”

In China, the experts spent half of their monthlong mission quarantined in hotels. Once released, they made one trip to the Wuhan Institute of Virology. Daszak later described the visit to *60 Minutes*: “We met with them. We said, ‘Do you audit the lab?’ And they said, ‘Annually.’ ‘Did you audit it after the outbreak?’ ‘Yes.’ ‘Was anything found?’ ‘No.’ ‘Do you test your staff?’ ‘Yes.’ No one was—”

The correspondent, Lesley Stahl, interrupted: “But you’re just taking their word for it.” Daszak responded, “Well, what else can we do? There’s a limit to what you can do and we went right up to that limit. We asked them tough questions.... And the answers they gave, we found to be believable—correct and convincing.”

On March 24, 2021, Daszak presented a confidential preview of the WHO mission's findings to a group of federal health and national security officials in a packed government conference room. Dressed in a tweed jacket instead of his usual hiking gear, he clicked through a 36-slide presentation, which *Vanity Fair* obtained.

Peter Daszak's 36-slide presentation summarizing the deliberations of the WHO-convened study on COVID-19's origins. [Click here](#) to see and download the full presentation.

Amid the charts, graphs, and old photos from the Huanan market of caged animals that could have harbored the virus, there was one slide devoted to the Wuhan Institute of Virology. It seemed to suggest that the questions swirling around the laboratory as a possible source of the pandemic could be put to rest. There had been annual external audits with no unusual findings.

Access was strictly controlled. And his trusted partner Shi Zhengli said there had been no COVID-like illnesses among her staff.

The presentation complete, Daszak held up his hands, as if waiting for a standing ovation, the attendee recounted: “His ego couldn’t fit in the room with all those interagency partners.”

The WHO Commission released its 120-page final report a week later. The experts had voted, by a show of hands, that direct transmission from bat to human was possible to likely; transmission through an intermediate animal was likely to very likely; transmission through frozen food was possible; and transmission through a laboratory incident was “extremely unlikely.”

The report was so error-riddled and unpersuasive that WHO director general Tedros effectively disowned it the day it was released. “As far as WHO is concerned all hypotheses remain on the table,” he said.

Three months later, the commission’s lead expert, Danish food scientist Peter Ben Embarek, extinguished the last embers of the report’s credibility. He confessed to a documentary film crew that the group had made a backroom deal with the 17 Chinese experts attached to the commission: The report could mention the lab-leak theory only “on the condition we didn’t recommend any specific studies to further that hypothesis” and used the phrase “extremely unlikely” to characterize it.

But that wasn’t the final shoe to drop. Daszak himself all but admitted—in a letter to Dr. Michael Lauer, the NIH’s deputy director for extramural research—that he had signed on to the WHO mission with a personal and professional agenda: to gather exculpatory information about the WIV, in part to help lift the curtain of suspicion around his grant so it could be reinstated.

“I have made extensive efforts to satisfy NIH’s broad concerns,” he wrote on April 11, 2021. “This includes serving as an expert on the WHO-China joint Mission on the Animal Origins of COVID-19, which involved 1 month on the ground in China (including 2 weeks locked in quarantine), at great personal burden and risk to me, to our organization, and to my family.”

He wrote that, while he had “acted in good faith” to follow the WHO’s directives for the mission, he had also gathered essential information that “specifically addresses” one of the demands the NIH had made as a condition of reinstating the grant: that he arrange for an outside inspection team to find out if the WIV had SARS-CoV-2 in its possession prior to December 2019. He’d returned with “categorical statements from WIV senior staff” that they did not have it prior to December 2019, he wrote, and had managed to get their assurances included in the WHO final report.

Unfortunately for Daszak, the NIH was unmoved. The grant remains suspended today.

**O**n February 25, 2022, a day before Worobey, Andersen, Garry, and their 15 coauthors rushed their preprints into the public domain, claiming “dispositive evidence” that SARS-CoV-2 originated from the Huanan market, China’s CDC published a preprint of its own that contained new data and pointed to a different conclusion. It revealed that, of the 457 swabs taken from 18 species of animals in the market, none contained any evidence of the virus. Rather, the virus was found in 73 swabs taken from around the market’s environment, all linked to human infections. Thus, while the samples proved the market served as an “amplifier” of viral spread, they did not prove the market was the source.

Meanwhile, an analysis published on March 16 in the medical journal *BMJ Global Health*, written by a group of Italian scientists and coauthored by Sergei Pond, cites a growing body of studies indicating that the virus may have been spreading worldwide for weeks, or even months, before the officially recognized start date of December 2019. If true, this would entirely upend the presumption of the market as the genesis of the pandemic.

“There are still a lot of credible questions that have not been answered,” says Pond. And with “no overwhelming evidence in either direction,” he adds, he is “puzzled as to why it’s necessary to push in one direction.” (Responding to written questions, Andersen said, “I have no particular stake in the idea that SARS-CoV-2 came from the market and not from virology research. The science speaks for itself and the evidence is clear.”)

Simon Wain-Hobson has his own hypothesis for what is taking place: The group of scientists pushing the claim of natural origin, he says, “want to show that virology is not responsible [for causing the pandemic]. That is their agenda.”

*Additional research by Rebecca Aydin and Stan Friedman.*

## **More Great Stories From *Vanity Fair***

- Can Ukrainian Freedom Fighters Stand Up to the Russian Military?
- Grimes on Music, Mars, and Her Secret New Baby With Elon Musk
- Trump Is Blowing a Gasket Over His Joke of a Social Media Network
- How the Atlanta Spa Shootings Tell a Story of America
- Inside the Succession Drama at Scholastic
- Trump Is Now Spitballing Ways to Launch More Russian War, Then “Sit Back and Watch”
- The Psychology Behind Putin’s War
- From the Archive: How a Once Faceless Putin Took Control of the World’s Largest Country
- Not a subscriber? Join *Vanity Fair* to receive full access to VF.com and the complete online archive now.

## **FY22 CWMD Posture Hearing**

- 05/04/2021 (HASC-ISO)
- Chairman Gallego opened the hearing by expressing his concern over a possible weaponized COVID-like virus. He also asked the panel about the quality of our CWMD efforts with allies like South Korea, India and Japan. Ranking Member Kelly highlighted the threat of poisoning from biological agents as evidenced by recent Russian activity and how we preserve or strengthen international norms in the chem/bio arena. He also asked specifically about DoD grant funding for EcoHealth Alliance and their subsequent work with the Wuhan Institute of Virology ~ a question DTRA also recently received from a separate group of Members. Other panelists raised questions on synthetic biology, Open Skies, and fentanyl. A good number of questions were deferred to a classified discussion or written response, including Rep. Waltz' inquiry on what CIED capabilities we are leaving behind in Afghanistan.
- *Rep. Ruben Gallego*
  - While COVID was not weaponized, it could be.
  - Concerned that we are not working closely enough with South Korea, India, and Japan on CWMD.
  - How efficiently is the CWMD mission being executed across the USG?
- *Rep. Trent Kelly*
  - Focused on biological weapons and poisoning incidents from Russia.
  - Questioned Biden budget could hamper investments in CWMD mission.
  - Eco Health Alliance funding for WIV.
  - What are you doing to preserve international norms on chem/bio to prevent further erosion of the norms?
- *Rep. Rick Larsen*
  - Synthetic biology, 3D printing.
  - Status of the Unity of Effort Council, what legacy systems are you looking at?
- *Rep. Austin Scott*
  - Gaps in ABMS in being able to pick up weapons that may be used against us.
  - Need to be less reliant on publicly traded companies for space launch. Problems with having to depending on the private sector during a time of war.
  - Not entirely comfortable with President's seeking to establish a DARPA-like initiative at NIH. Would prefer it be housed elsewhere.
- *Rep. Don Bacon*
  - Is Iran your #1 threat for proliferation?
  - What is the status of the Open Skies program?
- *Rep. Stephanie Murphy*
  - How is the USG tracking shipments from Asia of fentanyl?
  - Concerned about transnational criminal organizations.
- *Rep. Michael Waltz*
  - What CIED capabilities are we leaving behind in Afghanistan?

**From:**  
**To:**

(b)(6)

**Subject:**

HAC-D Defense Appropriations Markup Recap

**Date:**

Thursday, June 23, 2022 3:31:24 PM

Team, see below.

HAC-D conducted a lively markup of the defense appropriations bill in front of the full appropriations committee. The level of spending (\$761 billion mirroring the president's budget) was criticized by republicans as too low to meet the current threat environment, in addition to concerns about inflation. Chairwoman DeLauro stated that the Pentagon was actually well insulated from inflation due to the multiyear contracts inherently preferred by the DOD. The legislation was adopted including a managers package amendment and five additional individual amendments. Two of these approved individual amendments sponsored by Representative Reschenthaler (R - PA 14) were restrictions on funding the EcoHealth Alliance and the Wuhan Institute of Virology. Additionally repeal language for the 2001 and 2002 Authorizations of Military Force from Representative Lee (D - CA 13) were included in the markup. Amendments that were not adopted included stipulations on military leave to obtain an abortion, the usage of funds to close Guantanamo Bay prison complex, and an across the board pay raise for junior enlisted servicemembers.

V/R,

(b)(6)

DTRA Legislative Affairs

Email

(b)(6)

Phone: 571-616-6580

**From:**  
**To:**

(b)(6)

**Subject:**  
**Date:**

Hearing Binder  
Monday, March 14, 2022 5:40:58 PM

Team,

Within the FY23 CWMD hearing folder on SharePoint, I created a binder folder. In here we should put preparation documents for the ADIR. Eventually we'll put in the final statements from the other witnesses, Q&A, etc. Right now I have in there the following:

(b)(5)

LINK TO BINDER FOLDER

[https://dtra1portal.unet.dtra.mil/LA/Shared%20Documents/Forms/AllItems.aspx?](https://dtra1portal.unet.dtra.mil/LA/Shared%20Documents/Forms/AllItems.aspx?RootFolder=%2FLA%2FShared%20Documents%2FCongressional%20Hearings%2FFY23%20CWMD%20Posture%20Hearing%2FOther%20Binder%20Docs&FolderCTID=0x012000EA6C8E03C44BCC4F8150207E683C980E&View=%7B13B0EAB7%2D7D42%2D49FE%2DA9BE%2D9CA015F1E3A0%7D)

RootFolder=%2FLA%2FShared%20Documents%2FCongressional%20Hearings%2FFY23%20CWMD%20Posture%20Hearing%2FOther%20Binder%20Docs&FolderCTID=0x012000EA6C8E03C44BCC4F8150207E683C980E&View=%7B13B0EAB7%2D7D42%2D49FE%2DA9BE%2D9CA015F1E3A0%7D

(b)(6)

Legislative Liaison  
Defense Threat Reduction Agency

(b)(6)

**From:**

(b)(6)

**To:**

**Subject:**

LA A&S/OSD

**Date:**

Wednesday, January 19, 2022 11:14:00 AM

---

(b)(6)

Have we received any responses back from LA both A&S and OSD concerning the EcoHealth Alliance tasker?

(b)(6)

Division Chief, Integration Management Division

Defense Threat Reduction Agency (DTRA)

(b)(6)



# Congress of the United States

Washington, DC 20515

October 27, 2021

The Honorable Merrick B. Garland  
Attorney General  
U.S. Department of Justice  
950 Pennsylvania Avenue, NW  
Washington, D.C. 20530

Dear Attorney General Garland:

We have been investigating whether U.S. taxpayer dollars funded dangerous research into deadly pathogens in Wuhan, China. For more than a year, the National Institutes of Health (NIH) and Dr. Anthony Fauci, director of the NIH's National Institute of Allergy and Infectious Diseases (NIAID), have denied using taxpayer money to fund this type of research. However, a recent admission from the NIH reveals that EcoHealth Alliance, Inc. (EcoHealth), a NIAID grant recipient, may have violated federal law in its taxpayer-funded work on deadly pathogens.<sup>1</sup> We accordingly refer this matter to the Justice Department for investigation.

On June 1, 2014, EcoHealth received a \$3.7 million dollar grant from NIAID, entitled "Understanding the Risk of Bat Coronavirus Emergence."<sup>2</sup> Through this grant, EcoHealth sent more than \$600,000 to the Wuhan Institute of Virology (WIV) in Wuhan, China. Further, pursuant to this grant, EcoHealth was required to report to NIH and "immediately stop all experiments" if it created a virus that showed evidence of viral growth 1,000 percent that of the original virus.<sup>3</sup> Even if EcoHealth did not immediately report an experiment that met these parameters as required by the grant, EcoHealth would have to submit its annual progress report by September 30, 2019. EcoHealth failed on both counts.

On October 20, 2021, we received a letter from Dr. Lawrence Tabak, Principal Deputy Director of the NIH. According to Dr. Tabak, EcoHealth "failed" to properly and promptly report an experiment that violated the terms of the grant.<sup>4</sup> The grant required EcoHealth to report any experiment that creates, intentionally or otherwise, a new virus that is 1,000 percent more virulent than its progenitor.<sup>5</sup> In one experiment, EcoHealth did just that but subsequently failed to report it. EcoHealth subsequently failed to file an annual report until August 3, 2021, almost two years after it was required to do so.<sup>6</sup>

---

<sup>1</sup> Letter from Lawrence A. Tabak, Principal Deputy Director, U.S. Nat'l Inst. Of Health, to Hon. James Comer, Ranking Member, H. Comm. on Oversight & Reform (Oct. 20, 2021).

<sup>2</sup> Project Grant, Understanding the Risk of Bat Coronavirus Research, EcoHealth Alliance, Inc. (June 1, 2014).

<sup>3</sup> Letter from Hon. Francis Collins, Dir., Nat'l Insts. Of Health, to Hon. James Comer, Ranking Member, H. Comm. on Oversight & Reform (July 28, 2021).

<sup>4</sup> Letter from Lawrence A. Tabak, *supra* note 1.

<sup>5</sup> *Id.*

<sup>6</sup> Understanding the Risk of Bat Coronavirus Emergence, 5RO1AI110964-05 (June 6, 2018 – May 31, 2019).

The revelation in Dr. Tabak's letter raises the prospect about whether EcoHealth violated 18 U.S.C. § 1031 and committed a major fraud against the United States. Section 1031 states, in relevant part, "[w]hoever knowingly executes, or attempts to execute, any scheme or artifice with the intent to defraud the United States; or to obtain money or property by means of false or fraudulent pretenses, representations, or promises, in any grant . . . if the value of such grant . . . is \$1,000,000 or more shall . . . be fined not more than \$1,000,000, or imprisoned not more than 10 years, or both."<sup>7</sup> The section's prohibition includes "misrepresenting a project's status to continue receiving funds."<sup>8</sup>

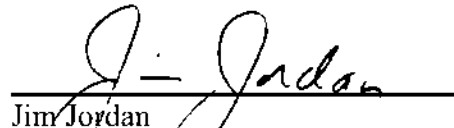
Between September 30, 2019 and August 3, 2021, EcoHealth received \$21,648,574 in grant funds from U.S. taxpayers that the company may not have received if it had timely disclosed to NIH that it had created a virus that would trigger the cessation of its experiments.<sup>9</sup> The fact that EcoHealth received more than \$21 million during this period shows that the company had a clear financial incentive to violate the terms of its grant by failing to stop its experiments. In addition, EcoHealth's failure to provide the required reporting to NIH for nearly two years—despite a requirement in the grant to do so annually—suggests that EcoHealth knowingly withheld information from NIH in an effort to misrepresent the project's status.

Based on the information available to us, we respectfully request that the Department of Justice investigate whether EcoHealth violated federal law by misrepresenting the status of its project to NIAID or NIH. Please respond by November 3, 2021 to inform us whether the Department intends to investigate this matter. Thank you for your attention to this matter.

Sincerely,



James Comer  
Ranking Member  
Committee on Oversight and Reform



Jim Jordan  
Ranking Member  
Committee on the Judiciary

cc: The Honorable Carolyn B. Maloney, Chairwoman  
Committee on Oversight and Reform

The Honorable Jerrold Nadler, Chairman  
Committee on the Judiciary

---

<sup>7</sup> 18 U.S.C. § 1031.

<sup>8</sup> *Grant Fraud Responsibilities*. Grants.gov (last accessed Oct. 21, 2021).

<sup>9</sup> USASpending.gov (last accessed Oct. 21, 2021).

<https://www.usaspending.gov/search/?hash=d664bf197193e61d56504abf646e5410>.

**From:**  
**To:**

(b)(6)

**Subject:**

NIH Admits to Funding Research in Wuhan, EcoHealth Violated Reporting

**Date:**

Tuesday, March 8, 2022 1:29:38 PM

**Attachments:**

2021-10-20 HHS EcoHealth ltr to Rep Comer.pdf  
Letter-to-DOJ-re.-EHA.pdf

..

(b)(5)

= = = = =

NIH Admits to Funding Gain-of-Function Research in Wuhan, Says EcoHealth Violated Reporting Requirements  
10/21/2021 | Caroline Downey | Yahoo News

A top NIH official admitted in a Wednesday letter that U.S. taxpayers funded gain-of-function research on bat coronaviruses in Wuhan and revealed that EcoHealth Alliance, the U.S. non-profit that funneled NIH money to the Wuhan Institute of Virology, was not transparent about the work it was doing.

In the letter to Representative James Comer (R-KY), Lawrence A. Tabak of the NIH cites a "limited experiment" that was conducted to test if "spike proteins from naturally occurring bat coronaviruses circulating in China were capable of binding to the human ACE2 receptor in a mouse model." The laboratory mice infected with the modified bat virus "became sicker" than those infected with the unmodified bat virus.

The revelation vindicates Republican senator Rand Paul, who got into heated exchanges with National Institute of Allergy and Infectious Disease director Anthony Fauci during his May and July testimonials before Congress over the gain-of-function question. At the second hearing, Paul accused Fauci of misleading Congress by denying that the U.S. had funded gain-of-function projects at the Wuhan Institute of Virology.

Gain-of-function research involves extracting viruses from animals and artificially engineering them in a laboratory to make them more transmissible or deadly to humans.

In keeping with Fauci's refusal to use "gain-of-function," Tabak avoids the term, though the work he described matches its commonplace definition precisely.

A previously unpublished EcoHealth grant proposal filed with NIAID, obtained by The Intercept, had already exposed that \$599,000 of the total grant to the Wuhan Institute of Virology was for research designed to make viruses more dangerous and/or infectious.

Dr. Richard Ebright, biosafety expert and professor of chemistry and chemical biology at Rutgers University, had previously rebutted Fauci's claim that the NIH "has not ever and does not now fund gain of function research in the Wuhan Institute of Virology [WIV]" as "demonstrably false."

Ebright told National Review that the NIH-financed work at the WIV "epitomizes" the definition of gain-of-function research, which deals with "enhanced potential pandemic pathogen (PPP)" or those pathogens "resulting from the enhancement of the transmissibility and/or virulence of a pathogen."

In addition to his admission that gain-of-function research was being conducted with NIH money, Tabak also revealed that EcoHealth failed to comply with its reporting responsibilities under the grant. EcoHealth was required to submit to a "secondary review" in the event of certain developments that might increase the danger associated with the research. So, when Wuhan researchers successfully bound a natural bat coronavirus to a human AC2 receptor in mice, they were supposed to inform the NIH, but they didn't.

Eco Health now has five days, according to Tabak, to submit to NIH "any and all unpublished data" relating to this award's project for compliance purposes.

The remainder of the document attempts to prove that the naturally occurring bat coronaviruses used in the 2014-2018 NIH grant experiments "are decades removed from SARS-CoV-2 evolutionarily," only sharing 96-97 percent of the genome.

At first, the Youth League helped promote the work on social media and organized public events to introduce people to Mr. Lin. Later, the Youth League, China's military and the Central Political and Legal Affairs Commission, a party committee that oversees the police, co-produced episodes.

The Youth League has tied up with celebrities, including Chinese rock stars and national athletes, to attract more eyeballs.

Mr. Lin, the Youth League, the military and the commission didn't respond to requests for comment.

Some Chinese parents said in interviews that they didn't mind the rise in patriotic content. Unlike in Hong Kong, where some parents are unnerved by an increase in patriotic behavior in schools and changes in textbooks, many in mainland China are apathetic about it.

One teacher said her students recognize propaganda and often sigh or make faces when encountering political texts. One study, though, suggests that at least some students are embracing the message.

The study, published in September by researchers from Shanxi University, found that Chinese teens born after 1998 are more patriotic than their predecessors. They cited an online survey of more than 580 teenagers in which more than 90% used terms such as "lucky" and "satisfied" to describe how they felt about growing up in China.

Young people realize China's power and are proud of it, the academics wrote, unlike earlier generations, who regarded China as a backward country and believed Western values could change it. Many even dreamed of moving to the West.

Charlie Hong, a schoolteacher in Chongqing, said that is no longer the case. When he asked his students if they would like to immigrate to a different country, he said, all except one said no.

*--Yoko Kubota and Jonathan Cheng contributed to this article*

[RETURN TO TOP](#)

#### **14. China Making it Harder to Solve the Mystery of Where Covid Began**

Bloomberg News, Dec. 30 (1600) | Not Attributed

In the year since seafood hawkers started appearing at Wuhan's hospitals sickened with a strange and debilitating pneumonia, the world has learned a lot about Covid-19, from the way it spreads to how to inoculate against the infection. Despite these advances, a chasm remains in our understanding of the virus that's killed nearly 2 million people and whipsawed the global economy: we still don't know how it began.

Where the pathogen first emerged and how it transmitted to humans is a stubborn mystery, one that's becoming more elusive with each passing month. Before the initial cluster among stall-holders at a produce market in central China, the trail largely goes cold, and the country the novel coronavirus hit first — the place many blame for unleashing the disease on an under-prepared world — now has little incentive to help find the true origin of the greatest public health emergency in a century.

China has effectively snuffed out Covid-19, thanks to stringent border curbs, mass testing and a surveillance network that allows infected people and their contacts to be tracked via mobile phone data. With the fight over the pandemic's source becoming an extension of the broader conflict between the world's two superpowers, China is now trying to revise the virus narrative from the beginning, and nowhere is that more evident than at the original epicenter: Wuhan.

Images of first responders dwarf the entrance to the city's bright red exhibition hall like heroes from Maoist-era propaganda posters: the police officer, the doctor, the soldier; their faces obscured by masks. Inside, a giant photo of a nurse's hands, inflamed and peeling, hangs over an army of mannequins in Hazmat suits. A 3D hologram of medics tending to a critical coronavirus patient is beamed over a real-life hospital bed, the beeps of a heart-rate monitor creating a sense of drama not lost on the college students shuffling past transfixed. Nearby, testing kits are sealed in clear display cases, labeled like artifacts from another time.

As the world continues to grapple with soaring death counts and mutated strains, China is already relegating the pandemic to its version of history.

The Battle Against Covid-19 Special Exhibition seeks to memorialize everything from mask-making machines and 2,000-bed temporary hospitals to lockdown haircuts and remote learning. A timeline at the entrance to the exhibit chronicles President Xi Jinping's virus actions in careful detail, starting on Jan. 7, when he ordered the country's leaders to contain the rapidly swelling outbreak and ending in September, when Xi gave a speech to bureaucrats in Beijing on how China tamed the coronavirus.

There's no mention of the Huanan seafood market, those first infections, or the public uproar over the government's cover-ups in the early days of the epidemic, when it hid the extent of human-to-human transmission and delayed taking action. Li Wenliang, the whistleblower doctor whose death from Covid-19 sparked the biggest backlash Beijing had seen in years, appears in a lineup of other Wuhan physicians felled by the virus, barely noticeable. For many Chinese, that anger has been replaced with a sense of pride, that their country bested a crisis that's all but defeated the U.S., leaving China stronger and on track — by at least one consultancy's estimate - to become the world's biggest economy five years earlier than previously predicted.

With the virus firmly contained — Wuhan has had no locally-transmitted cases since May — there's a growing push to dispel the idea that China was the ultimate source of the virus, known officially as

SARS-CoV-2. A foreign ministry spokesman has been espousing theories that link the virus to the U.S. military, and after a spate of cases in Chinese port and cold storage workers, state-backed media are claiming the virus could have entered the country on imported frozen food. They've also seized on research that suggests there were infections in the U.S. and Italy that pre-date those in Wuhan.

While some of these theories may have credence, the irony is that we may never know how and where the virus emerged. China has ignored appeals for an independent investigation into the virus's origin, hammering Australia with trade restrictions after it called for one. It's also stalled efforts by the World Health Organization to get top infectious diseases experts into Wuhan this year. That's prevented the painstaking epidemiological detective work — from probing samples of the city's wastewater, to checking patient specimens collected months before the outbreak appeared for early traces of the pathogen and undertaking tests at the food market itself — that could provide insight into the chain of events that brought the virus to the bustling capital of Hubei province, and how to stop it from happening again.

Now, with a WHO team focused on tracing the virus's origin hoping to visit Wuhan in January, and a crew commissioned by The Lancet medical journal also on the hunt, the city may not have much to reveal. Life is largely back to normal for Wuhan's 11 million people, the first to experience the lockdowns now shuttering parts of Europe and North America for a second time.

"These things are awfully hard to do retrospectively, even if all the evidence is still in place," said Robert Schooley, an infectious-diseases physician at the University of California, San Diego and editor-in-chief of the journal Clinical Infectious Diseases.

Located just 5 miles south of the exhibition center, the Huanan seafood market is partitioned off by eight-foot-high metal barricades, replete with pictures of tranquil rural scenes — bolted to the ground. Potted palm trees dot the perimeter of the multi-story building, site of the world's first known cluster of Covid-19. Until government cleaners swooped in in late 2019, to close, vacate and sanitize dozens of stalls, it was a key source of produce for locals and restaurants in central Wuhan. It was also reported by media including Agence France Presse to have sold a range of wild animals and their meat, from koalas and wolf pups to rats and palm civets, the cat-like animals suspected of being the conduit of the SARS virus between bats and humans, which led to a deadly outbreak in China in 2002 that subsequently spread to other parts of the world.

Now only eyeglass vendors line the sparsely filled aisles on Huanan's second floor, their diminished clientele carefully vetted by security guards. On a recent visit to the market, Bloomberg News reporters were warned away by plain-clothes officials and later, police.

Beyond the carefully constructed museum exhibits, few other signs of Wuhan's epic battle with the coronavirus exist. A makeshift hospital famously built in about two weeks to treat thousands of critical

patients has been shut down and boarded up. Two local women said they'd heard the site would be turned into apartments.

In Wuhan Tiandi, a shopping precinct that claims to have China's first outdoor food street with air conditioning, couples and families rugged up against the winter chill casually remove their face masks to eat and chat. When asked about the origins of the virus, most said it didn't start in the city.

For all of China's stonewalling, scientists suspect they could well be right.

The place a virus first infects a human isn't necessarily where it begins spreading efficiently among people, said Joel Wertheim, an associate professor of medicine at the University of California, San Diego, where he studies the evolution and epidemiology of infectious diseases. HIV, for instance, is thought to have originated in chimpanzees in southeastern Cameroon, but didn't begin spreading readily in people until it reached the city of Kinshasa, hundreds of miles away.

While researchers surmised early on that the horseshoe bat identified as the likely source of SARS could also have spawned SARS-CoV-2, how it crossed the species barrier to infect humans remains unclear. It's likely that precursors to this virus spilled over from their natural reservoir many times, but went extinct when infected individuals didn't transmit the virus to anyone, according to Wertheim. Eventually, the virus infected someone who passed it to multiple people, who also passed it on to others.

"You could have sort of these one-off, dead-end transmission chains until you get into Hubei province, which is where the epidemiological data says this is where it was spreading," Wertheim said. "And it seems to have seeded the rest of China from there, and then from China to the rest of the world."

Chinese scientists published the genetic sequence of the virus in January, a move that has allowed experts elsewhere to make some inroads into how this may have started. Wertheim and his colleagues studied SARS-CoV-2 virus genomes and the pace at which they mutated and diversified from the earliest known specimens in Wuhan. From mid-October to mid-November 2019 is the most plausible period in which the first case in people emerged, according to a pre-print of Wertheim's research released Nov. 24.

The question of how the pathogen got to central China is the subject of more debate. The coronaviruses most closely related to SARS-CoV-2 were found in bats in China's Yunnan province, some 1,000 miles southwest of Wuhan. The mountainous region borders Vietnam, Laos and Myanmar, all countries known to have sizable horseshoe bat populations.

"We can't rule out that the person who first got this virus was in Yunnan and then infected another person who hopped on a plane and went back to Wuhan after their vacation," said Michael Worobey,



head of ecology and evolutionary biology at the University of Arizona in Tucson, who worked with Wertheim on the timing of the first possible case.

Other scientists see a potential answer in outbreaks half a world away. Over the past few months, SARS-CoV-2 has exploded among mink populations in Europe and North America after the virus was introduced by infected humans, with which they share some respiratory-tract features. Millions of the semi-aquatic, carnivorous mammals, reared for their soft pelts, have been culled to purge the pathogen from farms where they have been linked to mutations in the coronavirus that some scientists said could pose a threat to vaccine efficacy.

“The mink scenario to me says, where you’ve got a large population of susceptible animals in the right conditions with a certain density, then this virus is just going to go right through it,” said Hume Field, an Australian wildlife epidemiologist who worked on the international probe that linked SARS to horseshoe bats and is a member of The Lancet’s Covid-19 origins task force.

Field discovered the source of a deadly virus that killed horses and their handlers in eastern Australia more than 20 years ago. After an exhaustive search, he eventually found Hendra virus originated in large fruit bats, known locally as flying foxes. The finding led scientists to understand what veritable virus treasure troves bats are. Besides his investigation into the origins of Hendra and SARS, Field has also helped trace the Nipah and Ebola Reston viruses back to bats.

Did SARS-CoV-2 jump directly from bats to humans, or did it spread to another animal — a so-called intermediate host — that then passed it on to people? Finding out is key to reducing the risk of secondary outbreaks and the emergence of new strains impervious to the Covid-19 vaccines now being rolled out around the world. The virus’s affinity with mink suggests wild animals from the same “mustelid” family, which includes weasels and ferrets, that interacted with coronavirus-carrying bats may have played an intermediary role, according to Field.

Mink resemble “a microcosm of what could have happened prior to Covid,” said Peter Daszak, a New York-based zoologist who is part of both the WHO and The Lancet teams trying to trace the virus’s origins. He theorizes that the virus went from horseshoe bats to people in Wuhan via wildlife that were sold in the city or people connected with that trade. In the wake of the outbreak, China said it curtailed the sale and consumption of wild animals, but the trade is difficult to police given how integral it is to cuisine and traditional medicines, particularly in the south.

Since bats don’t fly regularly from southern China to Wuhan, it’s more likely the virus was propagated in civets or other susceptible animals raised on farms for sale in the Huanan market, Daszak said. In the wild, coronaviruses spread across animal species via the fecal-oral route, such as when a civet eats fruit contaminated by bat droppings.

“We still don’t really know what animals were present in that market in the beginning,” he said. “It’s quite possible there are other animals in China that were infected.”

Finding out more from those who were there will be difficult, especially a year on. Scientists still don’t know the precise source of the Ebola virus, for example, nor how the H1N1 influenza virus that swept the world in 2009 jumped from pigs into people. It’s possible the origin of Covid-19 will never be found, George Gao, the director of China’s Center for Disease Control and Prevention, told the Xinhua news agency this week. “We looked for suspect animals in Wuhan, but found none.”

After the Huanan market was closed, some of its stallholders were relocated to the cavernous Sijimei food market on Wuhan’s northern outskirts. On a frigid day in mid-December, it was almost deserted of customers, but few vendors were willing to speak to Bloomberg about the events that took place 12 months earlier. A spice and condiment seller who said his family name was Xie, confirmed he’d moved from Huanan in March, but said he couldn’t remember anything that happened there. Shortly after, security guards appeared saying that foreign media were barred from filming.

The response was similar at a nearby open-air market, where other Huanan vendors had set up stalls. An attendant selling lamb carcasses confirmed the business moved there in March before he was told to shut up by his manager. Moments later, two guards appeared, saying any interviews should be cleared by the Communist Party.

Bloomberg has made multiple requests over the course of 2020 to interview key Chinese scientists, including both the director and chief epidemiologist at the country’s CDC, and the nation’s most experienced coronavirus expert, Shi Zhengli.

Shi — known as China’s “bat woman” for her intrepid, decade-long exploration and collection of viruses in bat-festooned caves — has been at the center of speculation about the source of SARS-CoV-2 since its first weeks. She operates a laboratory at the Wuhan Institute of Virology that studies some of the planet’s worst infectious disease threats. Its location in a peri-urban industrial area about 20 miles from the Huanan market has fueled theories that the virus either accidentally escaped from the lab or, more sinister, that it was genetically engineered and deliberately released.

Shi has said the genetic characteristics of the viruses she’s worked on don’t match SARS-CoV-2 and told the state-run China Daily newspaper in early February that she was willing to “bet my life” that the outbreak had “nothing to do with the lab.” Shi is also open to “any kind of visit” to rule it out, the BBC reported Dec. 22.

Still, in a vacuum of information, conspiracy theories have taken hold, with President Donald Trump — who has repeatedly referred to SARS-CoV-2 as the “Chinese virus” — a proponent of the lab hypothesis. He said as early as April that China may have “knowingly” unleashed the pathogen, and

the U.S. has criticized the country's lack of cooperation on tracing its source. For its part, China defends its work with the WHO. It's engaged with the body on origin-tracing in a "transparent" manner and WHO experts have been allowed to visit the country, Wang Wenbin, a foreign ministry spokesman, told reporters this month.

Field, who's also a science and policy adviser for EcoHealth Alliance, a New York-based nonprofit that works to prevent viral outbreaks around the world, said it's possible Chinese scientists are well advanced in their investigations, but fears any findings into how the virus originated — whether from China or elsewhere — will be clouded in "conspiracy cover-up talk."

"How do we make those broadly accepted to what now seems to be quite a cynical and politicized audience?"

It will likely require a level of openness China is showing no signs of embracing.

On a recent visit to the Wuhan Institute of Virology, security staff tried to stop a Bloomberg journalist from taking photographs and video from a public road outside. One guard stood in the way of the car until police arrived. Multiple requests to visit the infectious diseases lab were denied.

Outside the city's Battle Against Covid-19 exhibition, there are no restrictions on filming. Visitors take photos of each other popping their heads out of wooden silhouettes with holes in place of faces, the kind you see of cartoon characters at theme parks, though here it's doctors in protective suits and gloves.

Yang Feng, a 51-year-old retiree, said she found the exhibit cathartic, a reminder of everything her home town had been through, from the almost three-month lockdown to the 3,869 people who died. "I wanted to recap the history," she said. "Now, you can't tell Wuhan is a city that's been through the virus."

But Yang shakes her head when asked where she thinks Covid-19 originated.

"I don't know," she said. "I really don't know."

--Jason Gale, Emma O'Brien and Claire Che; With assistance from Jing Li

[RETURN TO TOP](#)

QUESTION FOIA RELEASE

(b)(5)



**From:** (b)(6)  
**To:**  
**Cc:**  
**Subject:** RE: CWMD Congressional Questions Document  
**Date:** Monday, April 4, 2022 11:26:31 AM  
**Attachments:** CWMD Hearing Q and A (24MAR22).docx

---

(b)(6)

Please see attached the pre-CWMD Hearing Q&A which DTRA directorates contributed to.

V/r,

(b)(6)

Legislative Liaison  
Defense Threat Reduction Agency

(b)(6)

-----Original Message-----

**From:** (b)(6)

(b)(6)

**Sent:** Monday, April 4, 2022 9:48 AM

**To:** (b)(6)

(b)(6)

**Subject:** CWMD Congressional Questions Document

Good morning Ma'am,

(b)(5)

Please let me know if you have any questions.

V/r,

(b)(6)

Military Assistant to the Director  
Operational Analysis Department (OI-OA)  
Defense Threat Reduction Agency (DTRA)  
Comr  
VOIP

(b)(6)

**From:**

(b)(6)

**To:**

**Subject:**

RE: DIR Staff Meeting

**Date:**

Thursday, January 20, 2022 12:16:09 PM

---

I would say this is all good

(b)(5)

(b)(5)

-----Original Message-----

**From:**

(b)(6)

**Sent:** Thursday, January 20, 2022 11:06 AM

**To:**

(b)(6)

**Subject:** DIR Staff Meeting

(b)(6)

Do you have anything that I can put out in the Directors MTG.

(b)(5)

(b)(6)

Division Chief, Integration Management Division  
Defense Threat Reduction Agency (DTRA)

(b)(6)

**From:** (b)(6)  
**To:**  
**Subject:** RE: Due Today: CATMS-130122-22C5 EcoHealth (PUBLIC HEALTH IMPLICATIONS OF FEDERAL FUNDING PROVIDED FOR CERTAIN VIROLOGICAL RESEARCH)  
**Date:** Friday, January 14, 2022 11:30:15 AM

Thank you ma'am.

(b)(6)  
Program Analyst/Task Manager  
Office of the Chief of Staff (CS)  
Defense Threat Reduction Agency

(b)(6)

Cubicle 4560B

Email: (b)(6)

-----Original Message-----

**From:** (b)(6)  
**To:** (b)(6)  
**Sent:** Friday, January 14, 2022 11:29 AM  
**Subject:** RE: Due Today: CATMS-130122-22C5 EcoHealth (PUBLIC HEALTH IMPLICATIONS OF FEDERAL FUNDING PROVIDED FOR CERTAIN VIROLOGICAL RESEARCH)

(b)(6)

Changes are being reviewed and response will be sent back to you shortly.

(b)(6)

Division Chief, Integration Management Division  
Defense Threat Reduction Agency (DTRA)

(b)(6)

-----Original Message-----

**From:** (b)(6)  
**Sent:** Friday, January 14, 2022 9:20 AM  
**To:** (b)(6)  
**Cc:** (b)(6); DTRA Ft Belvoir Org List DTRA Staff Actions <dtra.belvoir.org.list.dtra-staff-actions@mail.mil>  
**Subject:** FW: Due Today: CATMS-130122-22C5 EcoHealth (PUBLIC HEALTH IMPLICATIONS OF FEDERAL FUNDING PROVIDED FOR CERTAIN VIROLOGICAL RESEARCH)  
**Importance:** High

Ma'am --

(b)(6) forwarded me the attached documents and they need to have a DTRA LA review of the comments provided prior to sending forward to the ADIR.

Thank you,

(b)(6)

Program Analyst/Task Manager  
Office of the Chief of Staff (CS)  
Defense Threat Reduction Agency

(b)(6)

Cubicle 4560B

Email: (b)(6)

-----Original Message-----

From: (b)(6)

(b)(6)

Sent: Thursday, January 13, 2022 5:07 PM

To: (b)(6)

(b)(6)

Subject: Due Today: CATMS-130122-22C5 EcoHealth (PUBLIC HEALTH IMPLICATIONS OF FEDERAL FUNDING PROVIDED FOR CERTAIN VIROLOGICAL RESEARCH)

CS Team,

Coordination complete through LCO, but CATMS is down. You may be able to push the attached through part of the process manually?

V/r,

(b)(6)

Legislative Liaison  
Defense Threat Reduction Agency

(b)(6)

-----Original Message-----

From: (b)(6)

(b)(6)

Sent: Thursday, January 13, 2022 4:01 PM

To: (b)(6)

(b)(6)

Cc: (b)(6)

(b)(6)

OSD Pentagon OUSD A-S Mailbox Legislative and Congressional Oversight FO  
<osd.pentagon.ousd-a-s.mbx.legislative-and-congressional-oversight@mail.mil>  
Subject: RE: Due Today: CATMS-130122-22C5 EcoHealth (PUBLIC HEALTH IMPLICATIONS OF FEDERAL FUNDING PROVIDED FOR CERTAIN VIROLOGICAL RESEARCH)

Good Afternoon,

LCO coord and edits are attached. CATMS is down at the moment for me. Once



it is back up I will upload and complete the tasker.

Very Respectfully,

(b)(6)

GAO/OIG Audit Liaison

OUSD(A&S) | Legislative & Congressional Oversight (LCO)

(b)(6)

Pentagon 3D886

-----Original Message-----

From: (b)(6)

Sent: Thursday, January 13, 2022 10:02 AM

To: (b)(6)

(b)(6)

Cc: OSD Pentagon OASD LA Mailbox Coordinations

<osd.pentagon.oasd-la.mbx.coordinations@mail.mil> (b)(6)

(b)(6)

Subject: RE: Due Today: CATMS-130122-22C5 EcoHealth (PUBLIC HEALTH IMPLICATIONS OF FEDERAL FUNDING PROVIDED FOR CERTAIN VIROLOGICAL RESEARCH)

Hi (b)(6)

LCO can review today. Please task it to USA-LCO-FO, LA, and GC in CATMS.  
After coordination, task it to USA-Editors.

(b)(6)

Please review this package this morning.

Respectfully,

(b)(6)

Legislative Analyst

OUSD(A&S) | Legislative & Congressional Oversight

USG Mobile: (b)(6)

Pentagon | 3D886 (remote Mon.-Fri., in office as required)

-----Original Message-----

From: (b)(6)

(b)(6)

Sent: Thursday, January 13, 2022 9:16 AM

To: (b)(6)

(b)(6)

Cc: OSD Pentagon OASD LA Mailbox Coordinations

<osd.pentagon.oasd-la.mbx.coordinations@mail.mil>

Subject: Due Today: CATMS-130122-22C5 EcoHealth (PUBLIC HEALTH IMPLICATIONS OF FEDERAL FUNDING PROVIDED FOR CERTAIN VIROLOGICAL RESEARCH)

Importance: High

Gentlemen,

Can you please push the below tasker up the chain for action? USD(A&S) is expecting this tasker to be completed today. Awaiting sign off from Mr. Kausner. Tasker is CATMS-130122-22C5. Subject: Public Health Implications Of Federal Funding Provided For Certain Virological Research.

Thanks,

(b)(6)

A rectangular box with a black border, used to redact a signature. The text "(b)(6)" is written in the top-left corner of the box.

Legislative Liaison

Defense Threat Reduction Agency

(b)(6)

A rectangular box with a black border, used to redact a signature. The text "(b)(6)" is written in the top-left corner of the box.

**From:** (b)(6)  
**To:**  
**Cc:**  
**Subject:** RE: EcoHealth Alliance  
**Date:** Thursday, June 23, 2022 6:02:05 PM

---

Glad we could assist!

-----Original Message-----

**From:** (b)(6)  
(b)(6)  
**Sent:** Thursday, June 23, 2022 5:35 PM

**To:** (b)(6)  
(b)(6)  
**Cc:** (b)(6)

(b)(6)  
**Subject:** RE: EcoHealth Alliance

(b)(6)

This is great, thanks for the heavy lift on such short notice.

(b)(6)

Congressional Appropriations Liaison  
OUSD (Comptroller), Budget and Appropriations Affairs  
Office (b)(6) Pentagon 3D755  
Cell: (b)(6)

-----Original Message-----

**From:** (b)(6)  
(b)(6)  
**Sent:** Thursday, June 23, 2022 5:21 PM

**To:** (b)(6)  
(b)(6)  
**Cc:** (b)(6)

(b)(6)  
**Subject:** RE: EcoHealth Alliance

Sir,

(b)(5) My  
apologies for the piecemeal responses.

V/r,

(b)(6)

Legislative Liaison

Defense Threat Reduction Agency

(b)(6)

-----Original Message-----

From: (b)(6)

(b)(6)

Sent: Wednesday, June 22, 2022 7:47 AM

To: (b)(6)

(b)(6)

Cc: (b)(6)

Subject: RE: EcoHealth Alliance

Steve,

(b)(5)

(b)(6)

Congressional Appropriations Liaison

OUSD (Comptroller), Budget and Appropriations Affairs

Office: (b)(6)

Cell: (b)(6) Pentagon 3D755

-----Original Message-----

From: (b)(6)

(b)(6)

Sent: Tuesday, June 21, 2022 5:37 PM

To: (b)(6)

(b)(6)

Cc: (b)(6)

Subject: RE: EcoHealth Alliance

(b)(6)

Attached represents the grants that DTRA has awarded to EcoHealth Alliance over the past 8 years. Standing by for any followup.

V/r,

(b)(6)

Legislative Liaison

Defense Threat Reduction Agency

(b)(6)

-----Original Message-----

From: (b)(6)

(b)(6)

Sent: Tuesday, June 21, 2022 5:06 PM

To: (b)(6)

(b)(6)

Cc: (b)(6)

(b)(6)

Subject: RE: EcoHealth Alliance

(b)(6)

I need an answer to the below question today. Can you help me please? (b)(5)

(b)(5)

Response today, please.

(b)(6)

Congressional Appropriations Liaison

OUSD (Comptroller), Budget and Appropriations Affairs

Off: (b)(6)

Pentagon 3D755

Cel:

From: (b)(6)

Sent: Tuesday, June 21, 2022 3:57 PM

To: (b)(6)

Cc:

(b)(6)

Subject: FW: EcoHealth Alliance

(b)(6)

Can you help (b)(6) question below?

(b)(6)

Congressional Appropriations Liaison

OUSD (Comptroller), Budget and Appropriations Affairs

Office (b)(6) Pentagon 3D755

Cell

From: (b)(6)

<mail

Sent: Tuesday, June 21, 2022 3:39 PM

To: (b)(6)

(b)(6)

Subject: [Non-DoD Source] FW: EcoHealth Alliance

(b)(5)

Thank you,

(b)(6)

From: (b)(6)

(b)(6)

Sent: Tuesday, June 21, 2022 3:36 PM

To: (b)(6)

<m

OU

<m

Subject: RE: EcoHealth Alliance

(b)(5)

v/r

(b)(6)

Army Congressional Liaison (Appropriations) Pentagon 3E331

Office (b)(6)

Cell:

(b)(6)

Portfolio: Defense Health, Medical RDTE, Medical Procurement, Wounded Warriors

**\*\*Please only call my cell phone and not my office as I am currently teleworking until further notice\*\***

From:

<mail

Sent: Tuesday, June 21, 2022 12:53 PM

To:

(b)(6)

Subject: [Non-DoD Source] RE: EcoHealth Alliance

Thanks for the quick turn around.

From:

(b)(6)

Sent: Tuesday, June 21, 2022 12:52 PM

To:

(b)(6)

Subject: RE: EcoHealth Alliance

(b)(5)

From: (b)(6)

<mail

Sent: Tuesday, June 21, 2022 12:45 PM

To: (b)(6)

(b)(6)

Subject: [Non-DoD Source] EcoHealth Alliance

Importance: High

(b)(5)

(b)(6)

Response today, please.

Thank you,

(b)(6)

House Committee on Appropriations

Subcommittee on Defense

Office: (b)(6)



**From:** (b)(6)  
**To:**  
**Cc:**  
**Subject:** RE: Ecohealth Alliance Update by COB  
**Date:** Wednesday, August 24, 2022 1:55:59 PM

---

(b)(6)

(b)(5)

V/r,

(b)(6)

Analyst | Contract Support

Office of the Deputy Assistant Secretary of Defense for Chemical and  
Biological Defense  
Pentagon, Room 3C949A

Office (b)(6)  
NIPR:  
SIPR:

-----Original Message-----

**From:** (b)(6)

(b)(6)

**Sent:** Wednesday, August 24, 2022 1:37 PM

**To:** (b)(6)

**Cc:**

(b)(6)

**Subject:** RE: Ecohealth Alliance Update by COB

(b)(6)

Would you mind forwarding the follow-up email from the committee? I just want to plug it into our tasking system. Also, after we satisfy this follow-up request, any further inquiries we will likely want to setup a meeting with the PSM.

Thanks,

(b)(6)

(b)(6)

Legislative Liaison  
Defense Threat Reduction Agency

(b)(6)

-----Original Message-----

From: (b)(6)

Sent: Thursday, August 18, 2022 1:34 PM

To: (b)(6)

(b)(6)

Cc: (b)(6)

(b)(6)

Subject: Ecohealth Alliance Update by COB

Steve,

I hope this finds you doing well.

(b)(5)

(b)(5)

Please let me know if there's any way I can assist..

V/r,

(b)(6)

Analyst | Contract Support  
Office of the Deputy Assistant Secretary of Defense for Chemical and  
Biological Defense  
Pentagon, Room 3C949A  
Office (b)(6)  
NIPR:  
SIPR:

**From:**  
**To:**  
  
**Cc:**  
**Subject:**  
**Date:**

(b)(6)  
  
  
RE: Ecohealth alliance update  
Wednesday, August 24, 2022 12:45:05 PM

---

(b)(5) Thanks guys.

(b)(6)

-----Original Message-----

From: (b)(6)  
Sent: Wednesday, August 24, 2022 12:44  
To: (b)(6)  
(b)(6)

Subject: RE: Ecohealth alliance update

(b)(6)

(b)(5)  
(b)(5) I'll periodically check-in with the team to get more insight.

V/r,

(b)(6)

Legislative Liaison  
Defense Threat Reduction Agency

(b)(6)

-----Original Message-----

From: (b)(6)  
Sent: Tuesday, August 23, 2022 2:55 PM  
To: (b)(6)  
(US  
Cc:  
Subject: Re: Ecohealth alliance update

(b)(5)

From: (b)(6)  
Date: Thursday, August 18, 2022 at 4:03:53 PM  
To: (b)(6)  
OAS  
Cc:  
Subject: Ecohealth alliance update

(b)(6)

(b)(5)

V/r,

(b)(6)

Analyst | Contract Support

Office of the Deputy Assistant Secretary of Defense for Chemical and Biological Defense

Pentagon, Room 3C949A

Office: (b)(6)

NIPR:

SIPR:

(b)(6)

**From:** (b)(6)  
**To:** (b)(6)  
**Cc:**  
**Subject:** RE: EcoHealth HAC-D inquiry  
**Date:** Thursday, June 23, 2022 5:17:06 PM

---

(b)(6)

Great! Thanks for the quick turn on this!

V/r,

(b)(6)

Legislative Liaison  
Defense Threat Reduction Agency

(b)(6)

-----Original Message-----

**From:** (b)(6)  
**Sent:** Thursday, June 23, 2022 1:57 PM

**To:** (b)(6)

(b)(6)

**Cc:** (b)(6)

(b)(6)

**Subject:** RE: EcoHealth HAC-D inquiry

Hi (b)(6)

Completed spreadsheet attached.

Kind regards,

(b)(6)

Staff Director, Strategic Communication & Outreach  
Chemical/Biological Technologies Department  
Research & Development Directorate  
Defense Threat Reduction Agency  
COR: HDTRA1-19-C-0004  
COR: HDTRA1-21-C-0042  
COR: HDTRA1-21-C-0054

#### STATEMENT of LIMITATION of AUTHORITY

You are hereby notified that I am not a contracting officer. I DO NOT have the authority to direct you in any way to alter your contractual obligation. Further, if the Government, as a result of the information obtained from today's discussion DOES desire to alter your requirements, changes will be issued in writing and signed by the contracting officer. You should take no action on any change unless and until you receive such a contract

modification.

-----Original Message-----

From: (b)(6)

(b)(6)

Sent: Thursday, June 23, 2022 10:27 AM

To: (b)(6)

Cc:

(b)(6)

Subject: EcoHealth HAC-D inquiry

(b)(6)

(b)(5)

Thanks!

(b)(6)

Legislative Liaison

Defense Threat Reduction Agency

(b)(6)

**From:**

(b)(6)

**To:**

**Cc:**

**Subject:**

RE: EcoHealth Reply - Tasker: CATMS19112021M3TB6E | PUBLIC HEALTH IMPLICATIONS OF FEDERAL FUNDING PROVIDED FOR CERTAIN VIROLOGICAL RESEARCH

**Date:**

Wednesday, January 19, 2022 9:03:57 PM

---

(b)(6)

(b)(5)

V/r,

(b)(6)

Legislative Liaison

Defense Threat Reduction Agency

(b)(6)

**From:** (b)(6)  
**To:** (b)(6)  
**Cc:**  
**Subject:** RE: EcoHealth Reply - Tasker: CATMS19112021M3TB6E | PUBLIC HEALTH IMPLICATIONS OF FEDERAL FUNDING PROVIDED FOR CERTAIN VIROLOGICAL RESEARCH  
**Date:** Wednesday, January 19, 2022 9:52:34 PM

---

Hey (b)(6), welcome! Adding Betsy who does NCB for our team. We are mostly telecommuting during the elevated HPCON but hopefully it's lifted soon and we can get all meet up!

(b)(6)

A&S Team Chief, OSD(LA)  
Pentagon 3D844  
Office (b)(6)  
Mobile  
SIPR:

-----Original Message-----

**From:** (b)(6)  
**To:** (b)(6)  
**Sent:** Wednesday, January 19, 2022 12:29  
**Subject:** RE: EcoHealth Reply - Tasker: CATMS19112021M3TB6E | PUBLIC HEALTH IMPLICATIONS OF FEDERAL FUNDING PROVIDED FOR CERTAIN VIROLOGICAL RESEARCH

Hello (b)(6)

I wanted to quickly introduce myself as I recently joined the DTRA LA team in December. In the near future I would like to visit the Pentagon to meet you and the rest of the LA Team. Previous to my assignment at DTRA I worked in the Programs Division of the Army OCLL. Also, thank you in advance for any assistance you can provide in reference to Steve's questions concerning the CATMS19112021M3TB6E tasker and I look forward to meeting you.

(b)(6)

Division Chief, Integration Management Division  
Defense Threat Reduction Agency (DTRA)

(b)(6)

-----Original Message-----

**From:** (b)(6)  
**Sent:** Wednesday, January 19, 2022 12:13 PM  
**To:** (b)(6)



(b)(6)

Cc: (b)(6)

(b)(6)

Subject: RE: EcoHealth Reply - Tasker: CATMS19112021M3TB6E | PUBLIC HEALTH  
IMPLICATIONS OF FEDERAL FUNDING PROVIDED FOR CERTAIN VIROLOGICAL RESEARCH

Adding (b)(6) who took over for (b)(6) (who is back on the Hill)

These are all good points (b)(5)

(b)(5)

(b)(6)

A&S Team Chief, OSD(LA)

Pentagon 3D844

Office (b)(6)

Mobile

SIPR:

-----Original Message-----

From: (b)(6)

<(b)(6)>

Sent: Wednesday, January 19, 2022 11:54

To: (b)(6)

(b)(6)

Cc: (b)(6)

(b)(6)

Subject: EcoHealth Reply - Tasker: CATMS19112021M3TB6E | PUBLIC HEALTH  
IMPLICATIONS OF FEDERAL FUNDING PROVIDED FOR CERTAIN VIROLOGICAL RESEARCH  
Importance: High

(b)(6)

DTRA was tasked with the following item: CATMS19112021M3TB6E - PUBLIC HEALTH  
IMPLICATIONS OF FEDERAL FUNDING PROVIDED FOR CERTAIN VIROLOGICAL RESEARCH.

(b)(5)

(b)(5)

Please advise on a way forward.

Thanks,

(b)(6)

Legislative Liaison

Defense Threat Reduction Agency

(b)(6)

**From:** (b)(6)  
**To:** (b)(6)  
**Cc:**  
**Subject:** RE: EcoHealth Reply - Tasker: CATMS19112021M3TB6E | PUBLIC HEALTH IMPLICATIONS OF FEDERAL FUNDING PROVIDED FOR CERTAIN VIROLOGICAL RESEARCH  
**Date:** Thursday, January 20, 2022 8:36:00 AM

---

(b)(6)

Thank you for the introduction and I look forward to the opportunity to visit the Pentagon and the team.

////////////////////

(b)(6)

I look forward to meeting you as well and know that we will be working together as we near the upcoming CWMD hearing. I was told that there is a NCB Charter that will be released in the upcoming weeks. I look forward to reading so we can make sure we are in line and on message. Again, I look forward to talking and meeting you soon.

(b)(6)

Division Chief, Integration Management Division  
Defense Threat Reduction Agency (DTRA)

(b)(6)

-----Original Message-----

**From:** (b)(6)  
**Sent:** Wednesday, January 19, 2022 9:53 PM  
**To:** (b)(6)  
(b)(6)  
**Cc:** (b)(6)  
(b)(6)  
**Subject:** RE: EcoHealth Reply - Tasker: CATMS19112021M3TB6E | PUBLIC HEALTH IMPLICATIONS OF FEDERAL FUNDING PROVIDED FOR CERTAIN VIROLOGICAL RESEARCH

Hey (b)(6) welcome! Adding (b)(6) who does NCB for our team. We are mostly telecommuting during the elevated HPCON but hopefully it's lifted soon and we can get all meet up!

(b)(6)

A&S Team Chief, OSD(LA)  
Pentagon 3D844  
Office: (b)(6)  
Mobile  
SIPR: i

-----Original Message-----

From: (b)(6)

(b)(6)

Sent: Wednesday, January 19, 2022 12:29

To: (b)(6)

Subject: RE: EcoHealth Reply - Tasker: CATMS19112021M3TB6E | PUBLIC HEALTH  
IMPLICATIONS OF FEDERAL FUNDING PROVIDED FOR CERTAIN VIROLOGICAL RESEARCH

Hello (b)(6)

I wanted to quickly introduce myself as I recently joined the DTRA LA team in December. In the near future I would like to visit the Pentagon to meet you and the rest of the LA Team. Previous to my assignment at DTRA I worked in the Programs Division of the Army OCLL. Also, thank you in advance for any assistance you can provide in reference to Steve's questions concerning the CATMS19112021M3TB6E tasker and I look forward to meeting you.

(b)(6)

Division Chief, Integration Management Division  
Defense Threat Reduction Agency (DTRA)

(b)(6)

-----Original Message-----

From: (b)(6)

Sent: Wednesday, January 19, 2022 12:13 PM

To: (b)(6)

(b)(6)

Cc: (b)(6)

(b)(6)

Subject: RE: EcoHealth Reply - Tasker: CATMS19112021M3TB6E | PUBLIC HEALTH  
IMPLICATIONS OF FEDERAL FUNDING PROVIDED FOR CERTAIN VIROLOGICAL RESEARCH

Adding (b)(6) who took over for (b)(6) (who is back on the Hill)

These are all good points (b)(5)

(b)(5)

(b)(6)

A&S Team Chief, OSD(LA)

Pentagon 3D844

Office: (b)(6)

Mobile

SIPR:

-----Original Message-----

From: (b)(6)

(b)(6)

Sent: Wednesday, January 19, 2022 11:54

To: (b)(6)

(b)(6)

Cc: (b)(6)

(b)(6)

Subject: EcoHealth Reply - Tasker: CATMS19112021M3TB6E | PUBLIC HEALTH  
IMPLICATIONS OF FEDERAL FUNDING PROVIDED FOR CERTAIN VIROLOGICAL RESEARCH  
Importance: High

(b)(6)

and

(b)(6)

DTRA was tasked with the following item: CATMS19112021M3TB6E - PUBLIC HEALTH  
IMPLICATIONS OF FEDERAL FUNDING PROVIDED FOR CERTAIN VIROLOGICAL RESEARCH.

(b)(5)

Please advise on a way forward.

Thanks,

(b)(6)

Legislative Liaison

Defense Threat Reduction Agency

(b)(6)

**From:**  
**To:**  
**Cc:**

(b)(6)

**Subject:**  
**Date:**

RE: Follow up RFI from HSGAC - Permanent investigations Subcommittee  
Monday, May 2, 2022 2:10:40 PM

(b)(6)

Thanks, (b)(5)

I'll keep everyone in the loop if he has any feedback.

V/R,

(b)(6)

Special Assistant  
OASD - Legislative Affairs  
1300 Defense Pentagon  
Room: 3D844  
Office (b)(6)  
NIPR  
SIPR:

-----Original Message-----

From: (b)(6)

Sent: Monday, May 2, 2022 12:01 PM

To: (b)(6)

(b)(6)

Cc: (b)(6)

(b)(6)

Subject: RE: Follow up RFI from HSGAC - Permanent investigations Subcommittee

(b)(6)

In late 2021, the Senate Committee on Homeland Security and Governmental Affairs, Permanent Subcommittee on Investigations sent a letter to the Secretary of Defense regarding their examination of the public health implications of federal funding provided for virological research (TAB B). Specifically, the subcommittee requested:

- All research proposals or grant applications submitted by or on behalf of EcoHealth Alliance (EcoHealth) and/or the Wuhan Institute of Virology.
- All documents or communications sent by the Defense Threat Reduction Agency(DTRA) in response to any research proposal or grant application submitted by or on behalf of EcoHealth and/or the Wuhan Institute of Virology.

DTRA submitted their findings to ASD(NCB) and they were subsequently released to the subcommittee by Mr. Andrew Hunter, Performing the Duties of the Under Secretary of Defense for Acquisition and Sustainment (USD(A&S)), on February 25, 2022.

On March 28, 2022, the subcommittee requested additional information, specifically:

- All unfunded research proposals and grant applications by or on behalf of EcoHealth and/or Wuhan Institute of Virology.
- Clarify DoD's position on the alleged unfunded proposal for WIV, as the co-grantee.

(b)(5)

v/r

(b)(6)

Legislative & Congressional Oversight (LCO) Office  
Office of the Under Secretary of Defense  
for Acquisition and Sustainment

(b)(6)

-----Original Message-----

From: (b)(6)

Sent: Monday, May 2, 2022 10:59 AM

To: (b)(6)

CIV

(US

Cc:

(b)(6)

Subject: RE: Follow up RFI from HSGAC - Permanent investigations Subcommittee

All,

Bumping this up, for everyone's SA.

Today is the response date. HSGAC contacted LA this morning to follow-up. Standing by to transmit when received.

Thanks!

V/R,

(b)(6)

Special Assistant  
OASD – Legislative Affairs  
1300 Defense Pentagon  
Room: 3D844

Office: (b)(6)

NIPR:

SIPR:

-----Original Message-----

From: (b)(6)

Sent: Wednesday, April 20, 2022 3:57 PM

To: (b)(6)

CD

Cc:

(b)(6)

Subject: RE: Follow up RFI from HSGAC - Permanent investigations Subcommittee

(b)(6)

Yes, 2 May is good.

(b)(6)

FYSA for this RFI, DTRA will respond by 2 May.

v/r

(b)(6)

Legislative & Congressional Oversight (LCO) Office  
Office of the Under Secretary of Defense  
for Acquisition and Sustainment

(b)(6)

-----Original Message-----

From: (b)(6)

Sent: Wednesday, April 20, 2022 3:31 PM

To: (b)(6)

Cc:

(b)(6)

Subject: RE: Follow up RFI from HSGAC - Permanent investigations Subcommittee

CDR (b)(6)

Could DTRA possibly get an extension on this RFI until May 2nd? We have the data ready, but DTRA has a new Director and she requires a bit more time to get spun up on all manner of details.

Please Advise.

Thanks,

(b)(6)



(b)(6)

Legislative Liaison  
Defense Threat Reduction Agency

(b)(6)

-----Original Message-----

From: (b)(6)

Sent: Monday, March 28, 2022 10:13 AM

To: (b)(6)

(b)(6)

Cc: (b)(6)

(b)(6)

Subject: FW: Follow up RFI from HSGAC - Permanent investigations Subcommittee

DTRA,

This came in two weeks ago, I thought it was being worked by our Congressional person, but it was not.

Can you generate an answer to this RFI that I can send along?

V/r

(b)(6)

From: (b)(6)

Sent: Wednesday, March 16, 2022 2:33 PM

To: (b)(6)

(b)(6)

Cc: (b)(6)

(b)(6)

Subject: FW: Follow up RFI from HSGAC - Permanent investigations Subcommittee

(b)(6)

The attached response was sent to HSGAC and received a follow up RFI:

"The letter asked for all grants applications and proposals, which would include grants that may not have ultimately been funded. It does not appear that the unfunded proposal list is included in the attachment to this production. As I am sure you are aware, at least one such proposal that was allegedly not funded has been made public, and would have included the Wuhan Institute of Virology as a co-grantee. Is it DoD's position that no such grant proposal exists?"

Adding a little detail, the article referred is from Atlantic Article,

<https://www.theatlantic.com/science/archive/2021/09/lab-leak-pandemic-origins-even-messier/620209/>.

The project appears to be named DEFUSE.

Please provide a response by 22 March.

Thanks.

v/r

(b)(6)

Legislative & Congressional Oversight (LCO) Office  
Office of the Under Secretary of Defense  
for Acquisition and Sustainment

(b)(6)

From: (b)(6)

Sent: Wednesday, March 16, 2022 2:23 PM

To: (b)(6)

Cc:

(b)(6)

Subject: FW: Follow up RFI from HSGAC - Permanent Investigations Subcommittee

(b)(6)

This should go to NCB. They wrote the letter that Mr. Hunter signed out.

Respectfully,

(b)(6)

From: (b)(6)

(b)(6)

Sent: Friday, March 11, 2022 9:03 AM

To: (b)(6)

Cc:

(b)(6)

Subject: Follow up RFI from HSGAC - Permanent investigations Subcommittee

(b)(6)

The attached response was sent to HSGAC and received a follow up RFI:

"The letter asked for all grants applications and proposals, which would include grants that may not have ultimately been funded. It does not appear that the unfunded proposal list is included in the attachment to this production. As I am sure you are aware, at least one such proposal that was allegedly not funded has been made public, and would have included the Wuhan

Institute of Virology as a co-grantee. Is it DoD's position that no such grant proposal exists?"

Adding a little detail, the article referred is from Atlantic Article,  
<https://www.theatlantic.com/science/archive/2021/09/lab-leak-pandemic-origins-even-messier/620209/>.  
The project appears to be named DEFUSE.

Please provide a response by 18 March.

Thanks.

V/r

(b)(6)

Legislative & Congressional Oversight (LCO) Office  
Office of the Under Secretary of Defense  
for Acquisition and Sustainment

(b)(6)

From: (b)(6)

Sent: Monday, March 7, 2022 6:25 PM

To: (b)(6)

Cc:

(b)(6)

Subject: Follow up RFI from HSGAC - Permanent investigations Subcommittee

(b)(6)

We sent the attached response to HSGAC and received a follow up RFI:

The letter asked for all grants applications and proposals, which would include grants that may not have ultimately been funded. It does not appear that the unfunded proposal list is included in the attachment to this production. As I am sure you are aware, at least one such proposal that was allegedly not funded has been made public, and would have included the Wuhan Institute of Virology as a co-grantee. Is it DoD's position that no such grant proposal exists?

Not sure who this should go to for a response. I'd appreciate if you could forward as applicable.

V/r,

(b)(6)

I am turning over with my relief, CDR (b)(6) USN. Please copy him on all emails you send to me (b)(6)

(b)(6)

Special Assistant  
OASD - Legislative Affairs  
1300 Defense Pentagon  
Room: 3D844

Office (b)(6)

Cell:

NIPR

SIPR

**From:**  
**To:**  
**Cc:**

(b)(6)

**Subject:**

RE: Follow up RFI from HSGAC - Permanent investigations Subcommittee

**Date:**

Monday, May 2, 2022 5:15:00 PM

**Attachments:**

RE Follow up RFI from HSGAC - Permanent investigations Subcommittee (19.8 KB).msg

We are good on this for now.

(b)(5)

-----Original Message-----

From: (b)(6)

Sent: Monday, May 2, 2022 11:05 AM

To: (b)(6)

Cc:

DT

(b)(6)

Subject: FW: Follow up RFI from HSGAC - Permanent investigations Subcommittee

Morning CDR (b)(6)

Just checking that everything is good to go on this tasker.

(b)(6)

V/r,

(b)(6)

Staff Actions Program Manager

Office of the Chief of Staff

(b)(6)

Defense Threat Reduction Agency (DTRA)

Fort Belvoir, VA 22060-6201

-----Original Message-----

From: (b)(6)

Sent: Monday, May 2, 2022 10:59 AM

To: (b)(6)

CIV

(US

Cc:

(b)(6)

Subject: RE: Follow up RFI from HSGAC - Permanent investigations Subcommittee

All,

Bumping this up, for everyone's SA.

Today is the response date. HSGAC contacted LA this morning to follow-up. Standing by to transmit when received.

Thanks!

**From:**

(b)(6)

**Sent:**

Mon, 2 May 2022 14:10:38 -0400

**To:**

(b)(6)

(b)(6)

**Cc:**

(b)(6)

LTC USARMY DTRA OI (U

OASD LA (USA)

**Subject:**

RE: Follow up RFI from HSGAC - Permanent investigations Subcommittee

**Attachments:**

smime.p7s

(b)(6)

Thanks

(b)(5)

(b)(5)

I'll keep everyone in the loop if he has any feedback.

V/R,

(b)(6)

Special Assistant

OASD Legislative Affairs

1300 Defense Pentagon

Room: 3D844

Office (b)(6)

NIPR

SIPR:

-----Original Message-----

From: (b)(6)

Sent: Monday, May 2, 2022 12:01 PM

To: (b)(6)

(b)(6)

Cc:

(b)(6)

(b)(6)

Subject: RE: Follow up RFI from HSGAC - Permanent investigations Subcommittee

(b)(6)

In late 2021, the Senate Committee on Homeland Security and Governmental Affairs, Permanent Subcommittee on Investigations sent a letter to the Secretary of Defense regarding their examination of the public health implications of federal funding provided for virological research (TAB B). Specifically, the subcommittee requested:

- All research proposals or grant applications submitted by or on behalf of EcoHealth Alliance (EcoHealth) and/or

the Wuhan Institute of Virology.

- All documents or communications sent by the Defense Threat Reduction Agency(DTRA) in response to any research proposal or grant application submitted by or on behalf of EcoHealth and/or the Wuhan Institute of Virology.

DTRA submitted their findings to ASD(NCB) and they were subsequently released to the subcommittee by Mr. Andrew Hunter, Performing the Duties of the Under Secretary of Defense for Acquisition and Sustainment (USD(A&S)), on February 25, 2022.

On March 28, 2022, the subcommittee requested additional information, specifically:

- All unfunded research proposals and grant applications by or on behalf of EcoHealth and/or Wuhan Institute of Virology.
- Clarify DoD's position on the alleged unfunded proposal for WIV, as the co-grantee.

(b)(5)

v/r

(b)(6)

Legislative & Congressional Oversight (LCO) Office  
Office of the Under Secretary of Defense  
for Acquisition and Sustainment

(b)(6)

-----Original Message-----

From: (b)(6)

Sent: Monday, May 2, 2022 10:59 AM

To: (b)(6)

CIV

(US

Cc:

(b)(6)

Subject: RE: Follow up RFI from HSGAC - Permanent investigations Subcommittee

All,

Bumping this up, for everyone's SA.

Today is the response date. HSGAC contacted LA this morning to follow-up. Standing by to transmit when received.

Thanks!

V/R,

(b)(6)

(b)(6)

Special Assistant  
OASD – Legislative Affairs  
1300 Defense Pentagon  
Room: 3D844  
Office (b)(6)  
NIPR: [REDACTED]  
SIPR: [REDACTED]

-----Original Message-----

From (b)(6)

Sent: Wednesday, April 20, 2022 3:57 PM

To: (b)(6)

CD

Cc:

(b)(6)

Subject: RE: Follow up RFI from HSGAC - Permanent investigations Subcommittee

(b)(6)

Yes, 2 May is good.

(b)(6)

FYSA for this RFI, DTRA will respond by 2 May.

v/r

(b)(6)

Legislative & Congressional Oversight (LCO) Office  
Office of the Under Secretary of Defense  
for Acquisition and Sustainment

(b)(6)

-----Original Message-----

From (b)(6)

Sent: Wednesday, April 20, 2022 3:31 PM

To: (b)(6)

Cc:

(b)(6)

Subject: RE: Follow up RFI from HSGAC - Permanent investigations Subcommittee

CDR (b)(6) and (b)(6)

Could DTRA possibly get an extension on this RFI until May 2nd? We have the



data ready, but DTRA has a new Director and she requires a bit more time to get spun up on all manner of details.

Please Advise.

Thanks,

(b)(6)

Legislative Liaison  
Defense Threat Reduction Agency

(b)(6)

-----Original Message-----

From: (b)(6)

Sent: Monday, March 28, 2022 10:13 AM

To: (b)(6)

(b)(6)

Cc: (b)(6)

(b)(6)

Subject: FW: Follow up RFI from HSGAC - Permanent investigations Subcommittee

DTRA,

This came in two weeks ago

(b)(5)

(b)(5)

V/r

john

From: (b)(6)

Sent: Wednesday, March 16, 2022 2:33 PM

To: (b)(6)

(b)(6)

Cc: (b)(6)

(b)(6)

Subject: FW: Follow up RFI from HSGAC - Permanent investigations Subcommittee

(b)(6)

The attached response was sent to HSGAC and received a follow up RFI:

"The letter asked for all grants applications and proposals, which would include grants that may not have ultimately been funded. It does not appear

that the unfunded proposal list is included in the attachment to this production. As I am sure you are aware, at least one such proposal that was allegedly not funded has been made public, and would have included the Wuhan Institute of Virology as a co-grantee. Is it DoD's position that no such grant proposal exists?"

Adding a little detail, the article referred is from Atlantic Article, <https://www.theatlantic.com/science/archive/2021/09/lab-leak-pandemic-origins-even-messier/620209/>. The project appears to be named DEFUSE.

Please provide a response by 22 March.

Thanks.  
v/r

(b)(6)

Legislative & Congressional Oversight (LCO) Office  
Office of the Under Secretary of Defense  
for Acquisition and Sustainment

(b)(6)

From: (b)(6)

Sent: Wednesday, March 16, 2022 2:23 P.M.

To: (b)(6)

Cc:

(b)(6)

Subject: FW: Follow up RFI from HSGAC - Permanent investigations Subcommittee

(b)(6)

This should go to NCB. They wrote the letter that Mr. Hunter signed out.

Respectfully,

(b)(6)

From: (b)(6)

(b)(6)

Sent: Friday, March 11, 2022 9:03 AM

To: (b)(6)

Cc:

(b)(6)

Subject: Follow up RFI from HSGAC - Permanent investigations Subcommittee

(b)(6)

The attached response was sent to HSGAC and received a follow up RFI:

"The letter asked for all grants applications and proposals, which would include grants that may not have ultimately been funded. It does not appear that the unfunded proposal list is included in the attachment to this production. As I am sure you are aware, at least one such proposal that was allegedly not funded has been made public, and would have included the Wuhan Institute of Virology as a co-grantee. Is it DoD's position that no such grant proposal exists?"

Adding a little detail, the article referred is from Atlantic Article, <https://www.theatlantic.com/science/archive/2021/09/lab-leak-pandemic-origins-even-messier/620209/>. The project appears to be named DEFUSE.

Please provide a response by 18 March.

Thanks.

v/r

(b)(6)

Legislative & Congressional Oversight (LCO) Office  
Office of the Under Secretary of Defense  
for Acquisition and Sustainment

(b)(6)

From: (b)(6)  
Sent: Monday, March 7, 2022 6:25 PM  
To: (b)(6)  
Cc: (b)(6)  
Subject: Follow up RFI from HSGAC - Permanent investigations Subcommittee

(b)(6)

We sent the attached response to HSGAC and received a follow up RFI:

The letter asked for all grants applications and proposals, which would include grants that may not have ultimately been funded. It does not appear that the unfunded proposal list is included in the attachment to this production. As I am sure you are aware, at least one such proposal that was allegedly not funded has been made public, and would have included the Wuhan Institute of Virology as a co-grantee. Is it DoD's position that no such grant proposal exists?

Not sure who this should go to for a response. I'd appreciate if you could forward as applicable.

V/r,

(b)(6)

I am turning over with my relief, CDR (b)(6) USN. Please copy him on all emails you send to me: (b)(6)

(b)(6)

Special Assistant  
OASD - Legislative Affairs  
1300 Defense Pentagon  
Room: 3D844  
Office: (b)(6)  
Cell: 5  
NIPR:  
SIPR:

(b)(6)

Thanks. I have the DARPA information and added it to your explanation. I fed that back to PSM (b)(6) I'll keep everyone in the loop if he has any feedback.

V/R,

(b)(6)

Special Assistant  
OASD – Legislative Affairs  
1300 Defense Pentagon  
Room: 3D844  
Office: (b)(6)  
NIPR:  
SIPR:

-----Original Message-----

From: (b)(6)

Sent: Monday, May 2, 2022 12:01 PM

To: (b)(6)

(b)(6)

Cc: (b)(6)

(b)(6)

Subject: RE: Follow up RFI from HSGAC - Permanent investigations Subcommittee

(b)(6)

In late 2021, the Senate Committee on Homeland Security and Governmental Affairs, Permanent Subcommittee on Investigations sent a letter to the Secretary of Defense regarding their examination of the public health implications of federal funding provided for virological research (TAB B). Specifically, the subcommittee requested:

- All research proposals or grant applications submitted by or on behalf of EcoHealth Alliance (EcoHealth) and/or the Wuhan Institute of Virology.
- All documents or communications sent by the Defense Threat Reduction Agency(DTRA) in response to any research proposal or grant application submitted by or on behalf of EcoHealth and/or the Wuhan Institute of Virology.

DTRA submitted their findings to ASD(NCB) and they were subsequently released to the subcommittee by Mr. Andrew Hunter, Performing the Duties of the Under Secretary of Defense for Acquisition and Sustainment (USD(A&S)), on February 25, 2022.

On March 28, 2022, the subcommittee requested additional information, specifically:

- All unfunded research proposals and grant applications by or on behalf of EcoHealth and/or Wuhan Institute of Virology.
- Clarify DoD's position on the alleged unfunded proposal for WIV, as the co-grantee.

(b)(6)

v/r

(b)(6)

Legislative & Congressional Oversight (LCO) Office  
Office of the Under Secretary of Defense  
for Acquisition and Sustainment

(b)(6)

-----Original Message-----

From: (b)(6)

Sent: Monday, May 2, 2022 10:59 AM

To: (b)(6)

(b)(6)

Cc: (b)(6)

(b)(6)

Subject: RE: Follow up RFI from HSGAC - Permanent investigations Subcommittee

All,

Bumping this up, for everyone's SA.

Today is the response date. HSGAC contacted LA this morning to follow-up. Standing by to transmit when received.

Thanks!

V/R,

(b)(6)

Special Assistant  
OASD - Legislative Affairs  
1300 Defense Pentagon  
Room: 3D844

Office: (b)(6)  
NIPR:  
SIPR:

-----Original Message-----

From: (b)(6)

Sent: Wednesday, April 20, 2022 3:57 PM

To: (b)(6)

(b)(6)

Cc: (b)(6)

(b)(6)

Subject: RE: Follow up RFI from HSGAC - Permanent investigations Subcommittee

(b)(6)

Yes, 2 May is good.

(b)(6)

FYSA for this RFI, DTRA will respond by 2 May.

v/r

(b)(6)

Legislative & Congressional Oversight (LCO) Office  
Office of the Under Secretary of Defense  
for Acquisition and Sustainment

(b)(6)

-----Original Message-----

From: (b)(6)

Sent: Wednesday, April 20, 2022 3:31 PM

To: (b)(6)

Cc:

(b)(6)

Subject: RE: Follow up RFI from HSGAC - Permanent investigations Subcommittee

CDR (b)(6) and (b)(6)

Could DTRA possibly get an extension on this RFI until May 2nd? We have the data ready, but DTRA has a new Director and she requires a bit more time to get spun up on all manner of details.

Please Advise.

Thanks,

(b)(6)

Legislative Liaison  
Defense Threat Reduction Agency

(b)(6)

-----Original Message-----

From: (b)(6)

Sent: Monday, March 28, 2022 10:13 AM

To: (b)(6)

(b)(6)

Cc: (b)(6)

(b)(6)

Subject: FW: Follow up RFI from HSGAC - Permanent investigations Subcommittee

DTRA,

This came in two weeks ago,

(b)(5)

(b)(5)

V/r

(b)(6)

From: (b)(6)

Sent: Wednesday, March 16, 2022 2:33 PM

To: (b)(6)

(b)(6)

Cc: (b)(6)

(b)(6)

Subject: FW: Follow up RFI from HSGAC - Permanent investigations Subcommittee



(b)(6)

The attached response was sent to HSGAC and received a follow up RFI:

"The letter asked for all grants applications and proposals, which would include grants that may not have ultimately been funded. It does not appear that the unfunded proposal list is included in the attachment to this production. As I am sure you are aware, at least one such proposal that was allegedly not funded has been made public, and would have included the Wuhan Institute of Virology as a co-grantee. Is it DoD's position that no such grant proposal exists?"

Adding a little detail, the article referred is from Atlantic Article, <https://www.theatlantic.com/science/archive/2021/09/lab-leak-pandemic-origins-even-messier/620209/>.

The project appears to be named DEFUSE.

Please provide a response by 22 March.

Thanks.

v/r

(b)(6)

Legislative & Congressional Oversight (LCO) Office  
Office of the Under Secretary of Defense  
for Acquisition and Sustainment

(b)(6)

From: (b)(6)

Sent: Wednesday, March 16, 2022 2:23 PM

To: (b)(6)

Cc:

(b)(6)

Subject: FW: Follow up RFI from HSGAC - Permanent investigations Subcommittee

(b)(6)

This should go to NCB. They wrote the letter that Mr. Hunter signed out.

Respectfully,

(b)(6)

From: (b)(6)

(b)(6)

Sent: Friday, March 11, 2022 9:03 AM

To: (b)(6)

Cc:

(b)(6)

Subject: Follow up RFI from HSGAC - Permanent investigations Subcommittee

(b)(6)

The attached response was sent to HSGAC and received a follow up RFI:

"The letter asked for all grants applications and proposals, which would include grants that may not have ultimately been funded. It does not appear that the unfunded proposal list is included in the attachment to this production. As I am sure you are aware, at least one such proposal that was allegedly not funded has been made public, and would have included the Wuhan Institute of Virology as a co-grantee. Is it DoD's position that no such grant proposal exists?"

Adding a little detail, the article referred is from Atlantic Article, <https://www.theatlantic.com/science/archive/2021/09/lab-leak-pandemic-origins-even-messier/620209/>.

The project appears to be named DEFUSE.

Please provide a response by 18 March.

Thanks.

v/r

(b)(6)

(b)(6)

Legislative & Congressional Oversight (LCO) Office  
Office of the Under Secretary of Defense  
for Acquisition and Sustainment

(b)(6)

From: (b)(6)

Sent: Monday, March 7, 2022 6:25 PM

To: (b)(6)

Cc:

(b)(6)

Subject: Follow up RFI from HSGAC - Permanent investigations Subcommittee

(b)(6)

We sent the attached response to HSGAC and received a follow up RFI:

The letter asked for all grants applications and proposals, which would include grants that may not have ultimately been funded. It does not appear that the unfunded proposal list is included in the attachment to this production. As I am sure you are aware, at least one such proposal that was allegedly not funded has been made public, and would have included the Wuhan Institute of Virology as a co-grantee. Is it DoD's position that no such grant proposal exists?

(b)(5)

V/r,

(b)(6)

I am turning over with my relief, CDR (b)(6) USN. Please copy him on all emails you send to me: (b)(6)

(b)(6)

Special Assistant  
OASD - Legislative Affairs  
1300 Defense Pentagon  
Room: 3D844

Office: (b)(6)  
Cell: (b)(6)  
NIPR: (b)(6)  
SIPR: (b)(6)

---

**From:** (b)(6)  
**Sent:** Mon, 2 May 2022 14:10:38 -0400  
**To:** (b)(6)  
(b)(6)  
**Cc:** (b)(6)  
LTC USARMY DTRA OI (U  
OASD LA (USA)  
**Subject:** RE: Follow up RFI from HSGAC - Permanent investigations Subcommittee  
**Attachments:** smime.p7s

(b)(6)

Thanks. (b)(5)

(b)(5) I'll keep everyone in the loop if he has any feedback.

V/R,

(b)(6)

Special Assistant  
OASD – Legislative Affairs  
1300 Defense Pentagon  
Room: 3D844  
Office: (b)(6)  
NIPR: (b)(6)  
SIPR: (b)(6)

-----Original Message-----

From: (b)(6)  
Sent: Monday, May 2, 2022 12:01 PM  
To: (b)(6)  
(b)(6)  
Cc: (b)(6)  
(b)(6)

(Betsy) CIV OSD OASD LA (USA) <elizabeth.h.thompson16.civ@mail.mil>; Stucky, Michael S CIV OSD OUSD A-S (USA) <michael.s.stucky.civ@mail.mil>; Yuen, Ava CIV OSD OASD LA (USA) <ava.yuen.civ@mail.mil>  
Subject: RE: Follow up RFI from HSGAC - Permanent investigations Subcommittee

Tim,

In late 2021, the Senate Committee on Homeland Security and Governmental Affairs, Permanent Subcommittee on Investigations sent a letter to the Secretary of Defense regarding their examination of the public health implications of federal funding provided for virological research (TAB B). Specifically, the subcommittee requested:

- All research proposals or grant applications submitted by or on behalf of EcoHealth Alliance (EcoHealth) and/or the Wuhan Institute of Virology.
- All documents or communications sent by the Defense Threat Reduction Agency(DTRA) in response to any research proposal or grant application submitted by or on behalf of EcoHealth and/or the Wuhan Institute of Virology.

DTRA submitted their findings to ASD(NCB) and they were subsequently released to the subcommittee by Mr. Andrew Hunter, Performing the Duties of the Under Secretary of Defense for Acquisition and Sustainment (USD(A&S)), on February 25, 2022.

On March 28, 2022, the subcommittee requested additional information, specifically:

- All unfunded research proposals and grant applications by or on behalf of EcoHealth and/or Wuhan Institute of Virology.
- Clarify DoD's position on the alleged unfunded proposal for WIV, as the co-grantee.

(b)(5)

w/r  
(b)(6)

Legislative & Congressional Oversight (LCO) Office  
Office of the Under Secretary of Defense  
for Acquisition and Sustainment

(b)(6)

-----Original Message-----

From: (b)(6)

Sent: Monday, May 2, 2022 10:59 AM

To: (b)(6)

CI

(U)

Cc

(b)(6)

Subject: RE: Follow up RFI from HSGAC - Permanent investigations Subcommittee

All,

Bumping this up, for everyone's SA.

Today is the response date. HSGAC contacted LA this morning to follow-up. Standing by to transmit when received.

Thanks!

V/R,

(b)(6)

Special Assistant  
OASD Legislative Affairs  
1300 Defense Pentagon  
Room: 3D844  
Office (b)(6)  
NIPR:  
SIPR:

-----Original Message-----

From: (b)(6)

Sent: Wednesday, April 20, 2022 3:57 PM

To: (b)(6)

CD

Cc:

(b)(6)

Subject: RE: Follow up RFI from IISGAC - Permanent investigations Subcommittee

(b)(6)

Yes, 2 May is good.

(b)(6)

FYSA for this RFI, DTRA will respond by 2 May.

v/r

(b)(6)

Legislative & Congressional Oversight (LCO) Office  
Office of the Under Secretary of Defense  
for Acquisition and Sustainment

(b)(6)

-----Original Message-----

From: (b)(6)

Sent: Wednesday, April 20, 2022 3:31 PM

To: (b)(6)

Cc: (b)(6)

Subject: RE: Follow up RFI from HSGAC - Permanent investigations Subcommittee

CDR (b)(6) and (b)(6)

Could DTRA possibly get an extension on this RFI until May 2nd? We have the data ready, but DTRA has a new Director and she requires a bit more time to get spun up on all manner of details.

Please Advise.

Thanks,

(b)(6)

Legislative Liaison  
Defense Threat Reduction Agency

(b)(6)

-----Original Message-----

From: (b)(6)

Sent: Monday, March 28, 2022 10:13 AM

To: (b)(6)

(b)(6)

Cc: (b)(6)

(b)(6)

Subject: FW: Follow up RFI from HSGAC - Permanent investigations Subcommittee

DTRA,

This came in two weeks ago. (b)(5)

(b)(5)

V/r

(b)(6)

From: (b)(6)

Sent: Wednesday, March 16, 2022 2:33 PM

To: (b)(6)

(b)(6)

Cc: (b)(6)

(b)(6)

Subject: FW: Follow up RFI from HSGAC - Permanent investigations Subcommittee

(b)(6)

The attached response was sent to HSGAC and received a follow up RFI:

"The letter asked for all grants applications and proposals, which would include grants that may not have ultimately been funded. It does not appear that the unfunded proposal list is included in the attachment to this production. As I am sure you are aware, at least one such proposal that was allegedly not funded has been made public, and would have included the Wuhan Institute of Virology as a co-grantee. Is it DoD's position that no such grant proposal exists?"

Adding a little detail, the article referred is from Atlantic Article, <https://www.theatlantic.com/science/archive/2021/09/lab-leak-pandemic-origins-even-messier/620209/>. The project appears to be named DEFUSE.

Please provide a response by 22 March.

Thanks.

v/r

(b)(6)

Legislative & Congressional Oversight (LCO) Office  
Office of the Under Secretary of Defense  
for Acquisition and Sustainment

(b)(6)

From (b)(6)

Sent: Wednesday, March 16, 2022 2:23 PM

To (b)(6)

Cc (b)(6)

(b)(6)

Subject: FW: Follow up RFI from HSGAC - Permanent investigations Subcommittee

(b)(6)

This should go to NCB. They wrote the letter that Mr. Hunter signed out.

Respectfully,

(b)(6)

From: (b)(6)

(b)(6)



Sent: Friday, March 11, 2022 9:03 AM

To: (b)(6)

Cc:

(b)(6)

Subject: Follow up RFI from HSGAC - Permanent investigations Subcommittee

(b)(6)

The attached response was sent to HSGAC and received a follow up RFI:

"The letter asked for all grants applications and proposals, which would include grants that may not have ultimately been funded. It does not appear that the unfunded proposal list is included in the attachment to this production. As I am sure you are aware, at least one such proposal that was allegedly not funded has been made public, and would have included the Wuhan Institute of Virology as a co-grantee. Is it DoD's position that no such grant proposal exists?"

Adding a little detail, the article referred is from Atlantic Article,

<https://www.theatlantic.com/science/archive/2021/09/lab-leak-pandemic-origins-even-messier/620209/>.

The project appears to be named DEFUSE.

Please provide a response by 18 March.

Thanks.

v/r

(b)(6)

Legislative & Congressional Oversight (LCO) Office  
Office of the Under Secretary of Defense  
for Acquisition and Sustainment

(b)(6)

From: (b)(6)

Sent: Monday, March 1, 2022 6:25 PM

To: (b)(6)

Cc:

(b)(6)

Subject: Follow up RFI from HSGAC - Permanent investigations Subcommittee

(b)(6)

We sent the attached response to HSGAC and received a follow up RFI:

The letter asked for all grants applications and proposals, which would include grants that may not have ultimately been funded. It does not appear that the unfunded proposal list is included in the attachment to this production. As I am sure you are aware, at least one such proposal that was allegedly not funded has been made public, and would have included the Wuhan Institute of Virology as a co-grantee. Is it DoD's position that no such grant proposal exists?

(b)(5)

V/r

(b)(6)

I am turning over with my relief, CDR (b)(6) USN. Please copy him on all emails you send to me: (b)(6)

(b)(6)

Special Assistant  
OASD - Legislative Affairs  
1300 Defense Pentagon  
Room: 3D844  
Office: (b)(6)  
Cell: 1  
NIPR:  
SIPR:

V/R,

(b)(6)

Special Assistant  
OASD – Legislative Affairs  
1300 Defense Pentagon  
Room: 3D844  
Office: (b)(6)  
NIPR:  
SIPR:

-----Original Message-----

From: (b)(6)

Sent: Wednesday, April 20, 2022 5:37 PM

To: (b)(6)

CD

Cc:

(b)(6)

Subject: RE: Follow up RFI from HSGAC - Permanent investigations Subcommittee

(b)(6)

Yes, 2 May is good.

(b)(6)

FYSA for this RFI, DTRA will respond by 2 May.

v/r

(b)(6)

Legislative & Congressional Oversight (LCO) Office  
Office of the Under Secretary of Defense  
for Acquisition and Sustainment

(b)(6)

-----Original Message-----

From: (b)(6)

Sent: Wednesday, April 20, 2022 3:31 PM

To: (b)(6)

Cc:

(b)(6)

Subject: RE: Follow up RFI from HSGAC - Permanent investigations Subcommittee

CDR (b)(6) and (b)(6)

Could DTRA possibly get an extension on this RFI until May 2nd? We have the data ready, but DTRA has a new Director and she requires a bit more time to get spun up on all manner of details.

Please Advise.

Thanks,

(b)(6)

Legislative Liaison  
Defense Threat Reduction Agency

(b)(6)

-----Original Message-----

From: (b)(6)

Sent: Monday, March 28, 2022 10:13 AM

To: (b)(6)

(b)(6)

Cc: (b)(6)

(b)(6)

Subject: FW: Follow up RFI from HSGAC - Permanent investigations Subcommittee

DTRA,

This came in two weeks ago. (b)(5)

(b)(5)

V/r

(b)(6)

From: (b)(6)

Sent: Wednesday, March 16, 2022 2:33 PM

To: (b)(6)

(b)(6)

Cc: (b)(6)

(b)(6)

Subject: FW: Follow up RFI from HSGAC - Permanent investigations Subcommittee

(b)(6)

The attached response was sent to HSGAC and received a follow up RFI:

"The letter asked for all grants applications and proposals, which would

include grants that may not have ultimately been funded. It does not appear that the unfunded proposal list is included in the attachment to this production. As I am sure you are aware, at least one such proposal that was allegedly not funded has been made public, and would have included the Wuhan Institute of Virology as a co-grantee. Is it DoD's position that no such grant proposal exists?"

Adding a little detail, the article referred is from Atlantic Article, <https://www.theatlantic.com/science/archive/2021/09/lab-leak-pandemic-origins-even-messier/620209/>. The project appears to be named DEFUSE.

Please provide a response by 22 March.

Thanks.  
v/r

(b)(6)

Legislative & Congressional Oversight (LCO) Office  
Office of the Under Secretary of Defense  
for Acquisition and Sustainment

(b)(6)

From: (b)(6)

Sent: Wednesday, March 16, 2022 2:23 PM

To: (b)(6)

Cc:

(b)(6)

Subject: FW: Follow up RFI from HSGAC - Permanent investigations Subcommittee

(b)(6)

This should go to NCB. They wrote the letter that Mr. Hunter signed out.

Respectfully,

(b)(6)

From: (b)(6)

(b)(6)

Sent: Friday, March 11, 2022 9:03 AM

To: (b)(6)

Cc:

(b)(6)

Subject: Follow up RFI from HSGAC - Permanent investigations Subcommittee

(b)(6)

The attached response was sent to HSGAC and received a follow up RFI:

"The letter asked for all grants applications and proposals, which would include grants that may not have ultimately been funded. It does not appear that the unfunded proposal list is included in the attachment to this production. As I am sure you are aware, at least one such proposal that was allegedly not funded has been made public, and would have included the Wuhan Institute of Virology as a co-grantee. Is it DoD's position that no such grant proposal exists?"

Adding a little detail, the article referred is from Atlantic Article, <https://www.theatlantic.com/science/archive/2021/09/lab-leak-pandemic-origins-even-messier/620209/>. The project appears to be named DEFUSE.

Please provide a response by 18 March.

Thanks.

v/r

(b)(6)

Legislative & Congressional Oversight (LCO) Office  
Office of the Under Secretary of Defense  
for Acquisition and Sustainment

(b)(6)

From: (b)(6)

Sent: Monday, March 7, 2022 6:25 PM

To: (b)(6)

Cc:

(b)(6)

Subject: Follow up RFI from HSGAC - Permanent investigations Subcommittee

(b)(6)

We sent the attached response to HSGAC and received a follow up RFI:

The letter asked for all grants applications and proposals, which would include grants that may not have ultimately been funded. It does not appear that the unfunded proposal list is included in the attachment to this production. As I am sure you are aware, at least one such proposal that was allegedly not funded has been made public, and would have included the Wuhan Institute of Virology as a co-grantee. Is it DoD's position that no such grant proposal exists?

(b)(5)

V/r,  
(b)(6)

I am turning over with my relief, CDR (b)(6) USN. Please copy him on all emails you send to me (b)(6)

(b)(6)

Special Assistant  
OASD - Legislative Affairs  
1300 Defense Pentagon  
Room: 3D844  
Office (b)(6)  
Cell:  
NIPR  
SIPR

(b)(6)

**From:**  
**To:**  
**Cc:**

(b)(6)

**Subject:** RE: Follow up RFI from HSGAC - Permanent investigations Subcommittee  
**Date:** Monday, May 2, 2022 11:59:26 AM

---

Thanks, (b)(6) I'll cc you on my transmittal.

v/r

(b)(6)

Legislative & Congressional Oversight (LCO) Office  
Office of the Under Secretary of Defense  
for Acquisition and Sustainment

(b)(6)

-----Original Message-----

From: (b)(6)

Sent: Monday, May 2, 2022 11:57 AM

To: (b)(6)

Cc:

LT

A-S

(b)(6)

Subject: RE: Follow up RFI from HSGAC - Permanent investigations Subcommittee

(b)(5)

If there is anything further required, please let us know.

V/r,

(b)(6)

SAIC Contract Support Office of the  
Assistant Secretary of Defense for Nuclear, Chemical, and Biological Defense  
Programs OASD(NCB) Front Office

(b)(6)

-----Original Message-----

From: (b)(6)

Sent: Monday, May 2, 2022 11:37 AM

To: (b)(6)

CT

Cc:

CIV

Subject: RE: Follow up RFI from HSGAC - Permanent investigations Subcommittee



(b)(6)

This is what I am prepared to send back to LA (b)(5)

Let me know if you are ok with this and I'll send it and close this RFI from my books.

\*\*\*\*\*

(b)(5)

v/r

(b)(6)

Legislative & Congressional Oversight (LCO) Office  
Office of the Under Secretary of Defense  
for Acquisition and Sustainment

(b)(6)

-----Original Message-----

From: (b)(6)

Sent: Monday, May 2, 2022 10:59 AM

To: (b)(6)  
CIV  
(US  
Cc:

(b)(6)

Subject: RE: Follow up RFI from HSGAC - Permanent investigations Subcommittee

All,

Bumping this up, for everyone's SA.

Today is the response date. HSGAC contacted LA this morning to follow-up. Standing by to transmit when received.

Thanks!

V/R,

(b)(6)

Special Assistant  
OASD – Legislative Affairs  
1300 Defense Pentagon  
Room: 3D844  
Office: (b)(6)  
NIPR:  
SIPR:

-----Original Message-----

From: (b)(6)

Sent: Wednesday, April 20, 2022 3:57 PM

To: (b)(6)

CD

Cc:

(b)(6)

Subject: RE: Follow up RFI from HSGAC - Permanent investigations Subcommittee

(b)(6)

Yes, 2 May is good.

(b)(6)

FYSA for this RFI, DTRA will respond by 2 May.

v/r

(b)(6)

Legislative & Congressional Oversight (LCO) Office  
Office of the Under Secretary of Defense  
for Acquisition and Sustainment

(b)(6)

-----Original Message-----

From: (b)(6)

Sent: Wednesday, April 20, 2022 3:31 PM

To: (b)(6)

Cc:

(b)(6)

Subject: RE: Follow up RFI from HSGAC - Permanent investigations Subcommittee

CDR (b)(6) and (b)(6)

Could DTRA possibly get an extension on this RFI until May 2nd? We have the data ready, but DTRA has a new Director and she requires a bit more time to get spun up on all manner of details.

Please Advise.

Thanks,

(b)(6)

Legislative Liaison

Defense Threat Reduction Agency

(b)(6)

-----Original Message-----

From: (b)(6)

Sent: Monday, March 28, 2022 10:13 AM

To: (b)(6)

<c

DJ

Cc

(b)(6)

Subject: FW: Follow up RFI from HSGAC - Permanent investigations Subcommittee

DTRA,

This came in two weeks ago, I thought it was being worked by our Congressional person, but it was not.

Can you generate an answer to this RFI that I can send along?

V/r

(b)(6)

From: (b)(6)

Sent: Wednesday, March 16, 2022 2:33 PM

To: (b)(6)

(b)(6)

Cc: (b)(6)

(b)(6)

Subject: FW: Follow up RFI from HSGAC - Permanent investigations Subcommittee

(b)(6)

The attached response was sent to HSGAC and received a follow up RFI:

"The letter asked for all grants applications and proposals, which would include grants that may not have ultimately been funded. It does not appear that the unfunded proposal list is included in the attachment to this production. As I am sure you are aware, at least one such proposal that was allegedly not funded has been made public, and would have included the Wuhan Institute of Virology as a co-grantee. Is it DoD's position that no such grant proposal exists?"

Adding a little detail, the article referred is from Atlantic Article, <https://www.theatlantic.com/science/archive/2021/09/lab-leak-pandemic-origins-even-messier/620209/>. The project appears to be named DEFUSE.

Please provide a response by 22 March.

Thanks.  
v/r

(b)(6)

Legislative & Congressional Oversight (LCO) Office  
Office of the Under Secretary of Defense  
for Acquisition and Sustainment

(b)(6)

From: (b)(6)

Sent: Wednesday, March 16, 2022 2:23 PM

To: (b)(6)

Cc: (b)(6)

(b)(6)

Subject: FW: Follow up RFI from HSGAC - Permanent investigations Subcommittee

(b)(6)

This should go to NCB. They wrote the letter that Mr. Hunter signed out.

Respectfully,

(b)(6)

From: (b)(6)

(b)(6)

Sent: Friday, March 11, 2022 9:03 AM

To: (b)(6)

Cc:

(b)(6)

Subject: Follow up RFI from HSGAC - Permanent investigations Subcommittee

(b)(6)

The attached response was sent to HSGAC and received a follow up RFI:

"The letter asked for all grants applications and proposals, which would include grants that may not have ultimately been funded. It does not appear that the unfunded proposal list is included in the attachment to this production. As I am sure you are aware, at least one such proposal that was allegedly not funded has been made public, and would have included the Wuhan Institute of Virology as a co-grantee. Is it DoD's position that no such grant proposal exists?"

Adding a little detail, the article referred is from Atlantic Article,

<https://www.theatlantic.com/science/archive/2021/09/lab-leak-pandemic-origins-even-messier/620209/>

The project appears to be named DEFUSE.

Please provide a response by 18 March.

Thanks.

v/r

(b)(6)

Legislative & Congressional Oversight (LCO) Office  
Office of the Under Secretary of Defense  
for Acquisition and Sustainment

(b)(6)

From: (b)(6)

Sent: Monday, March 7, 2022 6:25 PM

To: (b)(6)

Cc:

(b)(6)

Subject: Follow up RFI from HSGAC - Permanent investigations Subcommittee

(b)(6)

We sent the attached response to HSGAC and received a follow up RFI:

The letter asked for all grants applications and proposals, which would include grants that may not have ultimately been funded. It does not appear that the unfunded proposal list is included in the attachment to this production. As I am sure you are aware, at least one such proposal that was allegedly not funded has been made public, and would have included the Wuhan Institute of Virology as a co-grantee. Is it DoD's position that no such grant proposal exists?

Not sure who this should go to for a response. I'd appreciate if you could forward as applicable.

V/r,

(b)(6)

I am turning over with my relief, CDR (b)(6) USN. Please copy him on all emails you send to me. (b)(6)

(b)(6)

Special Assistant  
OASD - Legislative Affairs  
1300 Defense Pentagon  
Room: 3D844

Off: (b)(6)

Cell

NIP

SIP

**From:** (b)(6)  
**To:** (b)(6)  
**Subject:** RE: HASC Transcript  
**Date:** Wednesday, February 23, 2022 10:00:19 AM  
**Attachments:** 2021 HASC CWMD posture hearing.pdf

---

(b)(6)

That transcript included some highlighting for the LA staff. Attached is a clean copy for Dr. Williams.

Thanks,

(b)(6)

Legislative Liaison  
Defense Threat Reduction Agency

(b)(6)

-----Original Message-----

**From:** (b)(6)

(b)(6)

**Sent:** Wednesday, February 23, 2022 7:14 AM

**To:** (b)(6)

(b)(6)

**Cc:** (b)(6)

(b)(6)

**Subject:** RE: HASC Transcript

Hello,

Happy to help. You can find a copy of the transcript at the link below.

[https://dtralportal.unet.dtra.mil/LA/\\_layouts/15/WopiFrame2.aspx?sourcedoc={434297EE-C1DE-4A22-A84C-1F226F782801}&file=2021-05-04%20HASC-ISO%20CWMD%20posture%20hearing.docx&action=default](https://dtralportal.unet.dtra.mil/LA/_layouts/15/WopiFrame2.aspx?sourcedoc={434297EE-C1DE-4A22-A84C-1F226F782801}&file=2021-05-04%20HASC-ISO%20CWMD%20posture%20hearing.docx&action=default)

(b)(6)

Chief, Legislative Affairs  
Defense Threat Reduction Agency

(b)(6)

-----Original Message-----

**From:** (b)(6)  
**To:** (b)(6)  
**Subject:** RE: Last Year's HASC CWMD Hearing QFRs  
**Date:** Friday, February 25, 2022 9:44:00 AM  
**Attachments:** Dr. Williams QFRs for HASC-ISO CWMD Hearing (6.7.21).docx

---

(b)(6)

Please see attached QFRs from the previous CWMD Hearing. Please note that the last page is a DTRA recommended response to a question that was addressed to Ms. Walsh. Please let me know if you need anything else.

(b)(6)

Chief, Legislative Affairs  
Defense Threat Reduction Agency

(b)(6)

-----Original Message-----

**From:** (b)(6)

(b)(6)

**Sent:** Friday, February 25, 2022 9:04 AM

**To:** (b)(6)

(b)(6)

**Subject:** RE: Last Year's HASC CWMD Hearing QFRs

Thank you, ma'am!

(b)(6)

Special Assistant - Policy  
OSD Legislative Affairs | 3D844

Com (b)(6)

Mob (b)(6)

NIPR (b)(6)

SIPR (b)(6)

-----Original Message-----

**From:** (b)(6)

(b)(6)

**Sent:** Friday, February 25, 2022 9:03 AM

**To:** (b)(6)

(b)(6)



(b)(6)

Subject: RE: Last Year's HASC CWMD Hearing QFRs

(b)(6)

Let me do some research to see if I can locate them.

(b)(6)

Chief, Legislative Affairs  
Defense Threat Reduction Agency

(b)(6)

-----Original Message-----

From: (b)(6)

<caroline.d.jones3.vol@mail.mil>

Sent: Thursday, February 24, 2022 6:10 PM

To: (b)(6)

(b)(6)

Subject: Last Year's HASC CWMD Hearing QFRs

Hi CWMD hearing team,

I got an email from HASC-ISO subcommittee a few weeks ago asking if I could  
resend the QFRs from last year's CWMD posture hearing (b)(5)

(b)(5)

Thanks,

(b)(6)

Special Assistant - Policy

OSD Legislative Affairs | 3D844

Comm: (b)(6)

Mobil

(b)(6)

NIPR:

SIPR:

**From:**  
**To:**

(b)(6)

**Subject:**

RE: Rep Reschenthaler Submitting Amendments for EcoHealth Alliance

**Date:**

Wednesday, June 22, 2022 3:34:05 PM

I read through the amendments and they are similar to the ones he offered last year. Both were adopted by voice.

(#1) Prohibits funding to support any activity conducted by, or associated with, the Wuhan Institute of Virology.

(#2) Prohibits funding EcoHealth Alliance if such work is performed in China. Waivers are permitted.

-----Original Message-----

**From:**

(b)(6)

**Sent:** Wednesday, June 22, 2022 2:31 PM

**To:**

(b)(6)

(b)(6)

**Subject:** Rep Reschenthaler Submitting Amendments for EcoHealth Alliance

So far two different amendments and they have both been accepted.

(b)(6)

DTRA Legislative Affairs

**Email:**

(b)(6)

**Phone:**

**From:** (b)(6)  
**To:**  
**Cc:**  
**Subject:** RE: Review of EcoHealth activities  
**Date:** Thursday, August 18, 2022 7:48:06 AM

---

(b)(6)

I need to update my iPhone. So, I sent it this morning and forwarded to the LTC and LT as well.

(b)(6)

Inspector General  
Defense Threat Reduction Agency

(O) (b)(6)  
(C)

-----Original Message-----

**From:** (b)(6)  
(b)(6)  
**Sent:** Wednesday, August 17, 2022 3:58 PM

**To:** (b)(6)

**Cc:**

(b)(6)

**Subject:** Review of EcoHealth activities

Mr. (b)(6)

I wanted to follow-up on our EcoHealth discussion from yesterday.

(b)(5)

(b)(5)

Thanks!

(b)(6)

Legislative Liaison  
Defense Threat Reduction Agency

(b)(6)

**From:** (b)(6)  
**To:**  
**Subject:** RE: Tasker: CATMS19112021M3TB6E - PUBLIC HEALTH IMPLICATIONS OF FEDERAL FUNDING PROVIDED FOR CERTAIN VIROLOGICAL RESEARCH  
**Date:** Wednesday, January 5, 2022 3:11:10 PM

This tasker on EcoHealth is getting further bogged down. See below.

-----Original Message-----

**From:** (b)(6)  
**Sent:** Wednesday, January 5, 2022 1:29 PM  
**To:** (b)(6)  
**Subject:** RE: Tasker: CATMS19112021M3TB6E - PUBLIC HEALTH IMPLICATIONS OF FEDERAL FUNDING PROVIDED FOR CERTAIN VIROLOGICAL RESEARCH

(b)(6)

There are two separate taskers and I am waiting to hear from CB (b)(5)

(b)(5)

(b)(6)

-----Original Message-----

**From:** (b)(6)  
**Sent:** Wednesday, January 5, 2022 1:27 PM  
**To:** (b)(6)  
**Cc:** (b)(6)  
**Subject:** Tasker: CATMS19112021M3TB6E - PUBLIC HEALTH IMPLICATIONS OF FEDERAL FUNDING PROVIDED FOR CERTAIN VIROLOGICAL RESEARCH

(b)(6)

See below. Have you seen any traffic about this tasker getting extended by a few days?

Thanks,

(b)(6)

-----Original Message-----

**From:** (b)(6)  
**Sent:** Wednesday, January 5, 2022 10:15 AM  
**To:** (b)(6)  
**Cc:** (b)(6)  
**Subject:** PUBLIC HEALTH IMPLICATIONS OF FEDERAL FUNDING PROVIDED FOR CERTAIN VIROLOGICAL RESEARCH

Hi (b)(6)

Just a note that (b)(6) touched base with (b)(6) office who issued this task, it will be extended to 11 Jan. It may not float down through CATMS yet, but if you could let the 4th floor know that'd be great.

Thanks

(b)(6)

-----Original Message-----

From: (b)(6)

(b)(6)

Sent: Wednesday, January 5, 2022 9:28 AM

To: (b)(6)

Subject: Tasker: CATMS19112021M3TB6E - PUBLIC HEALTH IMPLICATIONS OF FEDERAL FUNDING PROVIDED FOR CERTAIN VIROLOGICAL RESEARCH

BACKGROUND: The Senate Homeland Security Committee has asked for information related to DTRA's work with EcoHealth Alliance. They've requested: (1) All research proposals or grant applications submitted by or on behalf of EcoHealth Alliance and/or the Wuhan Institute of Virology, and (2) All documents or communications sent by the agency in response to any research proposal or grant application submitted by or on behalf of EcoHealth and/or the WIV.

ACTION: Please review the files placed in supporting documents to determine if they are sufficient to answer the committee's request. Said data was provided to HASC on a similar question in August. If other, please add and advise.

SUSPENSE: 6 Jan 2021

**From:** (b)(6)  
**To:** (b)(6)  
**Cc:** (b)(6); DTRA Ft Belvoir Org List DTRA Staff Actions (b)(6)  
**Subject:** CIV DTRA DIR (USA)  
RE: Tasker: CATMS19112021M3TB6E - PUBLIC HEALTH IMPLICATIONS OF FEDERAL FUNDING PROVIDED FOR CERTAIN VIROLOGICAL RESEARCH  
**Date:** Thursday, January 6, 2022 12:54:44 PM

(b)(6)

Thanks for the update.

(b)(5)

V/r,

(b)(6)

Legislative Liaison  
Defense Threat Reduction Agency

(b)(6)

-----Original Message-----

**From:** (b)(6)

(b)(6)

**Sent:** Thursday, January 6, 2022 8:19 AM

**To:** (b)(6)

(b)(6)

**Cc:** (b)(6)

(b)(6)

; DTRA Ft Belvoir Org List DTRA Staff

Actions <dtra.belvoir.org.list.dtra-staff-actions@mail.mil> (b)(6)

(b)(6)

**Subject:** RE: Tasker: CATMS19112021M3TB6E - PUBLIC HEALTH IMPLICATIONS OF FEDERAL FUNDING PROVIDED FOR CERTAIN VIROLOGICAL RESEARCH

(b)(6)

So this is where things get interesting:

CATMS19112021M3TB6E came in from NCB. (b)(5)

(b)(5)

CATMS-040122-F699 came in from ASD/CBD requesting all the same info as the task above. (b)(5)

(b)(5)

I can send that other task to you to load the inputs from DTRA-210817-TDTK (which is the exact same result) and we can let NCB deal with the duplication if you would rather push that way. Seems that RD is already tracking that so either way it works for me.

Rinse and repeat...this subject doesn't seem to be going away anytime soon.

(b)(6)

-----Original Message-----

From: (b)(6)

(b)(6)

Sent: Wednesday, January 5, 2022 3:05 PM

To: (b)(6)

(b)(6)

Cc: (b)(6)

(b)(6)

Subject: RE: Tasker: CATMS19112021M3TB6E - PUBLIC HEALTH IMPLICATIONS OF  
FEDERAL FUNDING PROVIDED FOR CERTAIN VIROLOGICAL RESEARCH

This tasker on EcoHealth is getting further bogged down. See below.

-----Original Message-----

From: (b)(6)

(b)(6)

Sent: Wednesday, January 5, 2022 1:29 PM

To: (b)(6)

(b)(6)

Subject: RE: Tasker: CATMS19112021M3TB6E - PUBLIC HEALTH IMPLICATIONS OF  
FEDERAL FUNDING PROVIDED FOR CERTAIN VIROLOGICAL RESEARCH

(b)(6)

There are two separate taskers and I am waiting to hear from CB (why are we  
giving them information when we are giving information to NCB direct). I  
haven't heard back from A&S but I will ask the question.

(b)(6)

-----Original Message-----

From: (b)(6)

(b)(6)

Sent: Wednesday, January 5, 2022 1:27 PM

To: (b)(6)

(b)(6)

Cc: (b)(6)

(b)(6)

Subject: Tasker: CATMS19112021M3TB6E - PUBLIC HEALTH IMPLICATIONS OF FEDERAL  
FUNDING PROVIDED FOR CERTAIN VIROLOGICAL RESEARCH

(b)(6)

See below. Have you seen any traffic about this tasker getting extended by a  
few days?

Thanks,

(b)(6)

-----Original Message-----



From: (b)(6)

(b)(6)

Sent: Wednesday, January 5, 2022 10:15 AM

To: (b)(6)

Cc:

(b)(6)

Subject: PUBLIC HEALTH IMPLICATIONS OF FEDERAL FUNDING PROVIDED FOR CERTAIN  
VIROLOGICAL RESEARCH

Hi (b)(6)

Just a note that (b)(6) touched base with (b)(6) office who issued  
this task, it will be extended to 11 Jan. It may not float down through  
CATMS yet, but if you could let the 4th floor know that'd be great.

Thanks

(b)(6)

-----Original Message-----

From: (b)(6)

(b)(6)

Sent: Wednesday, January 5, 2022 9:28 AM

To: (b)(6)

Subject: Tasker: CATMS19112021M3TB6E - PUBLIC HEALTH IMPLICATIONS OF FEDERAL  
FUNDING PROVIDED FOR CERTAIN VIROLOGICAL RESEARCH

BACKGROUND: The Senate Homeland Security Committee has asked for information  
related to DTRA's work with EcoHealth Alliance. They've requested: (1) All  
research proposals or grant applications submitted by or on behalf of  
EcoHealth Alliance and/or the Wuhan Institute of Virology, and (2) All  
documents or communications sent by the agency in response to any research  
proposal or grant application submitted by or on behalf of EcoHealth and/or  
the WIV.

(b)(5)

SUSPENSE: 6 Jan 2021

**From:** (b)(6)  
**To:** (b)(6)  
**Cc:** (b)(6); DTRA Ft Belvoir Org List DTRA Staff Actions (b)(6)  
**Subject:** RE: Tasker: CATMS19112021M3TB6E - PUBLIC HEALTH IMPLICATIONS OF FEDERAL FUNDING PROVIDED FOR CERTAIN VIROLOGICAL RESEARCH  
**Date:** Thursday, January 6, 2022 8:19:11 AM

..

(b)(6)

So this is where things get interesting:

CATMS19112021M3TB6E came in from NCB. Same inputs as previous tasks, which is basically anything that we granted to EcoHealth.

CATMS-040122-F699 came in from ASD/CBD requesting all the same info as the task above. (b)(5)

(b)(5)

I can send that other task to you to load the inputs from DTRA-210817-TDTK (which is the exact same result) and we can let NCB deal with the duplication if you would rather push that way. Seems that RD is already tracking that so either way it works for me.

Rinse and repeat...this subject doesn't seem to be going away anytime soon.

(b)(6)

-----Original Message-----

**From:** (b)(6)  
(b)(6)  
**Sent:** Wednesday, January 5, 2022 3:05 PM  
**To:** (b)(6)  
(b)(6)  
**Cc:** (b)(6)  
(b)(6)  
**Subject:** RE: Tasker: CATMS19112021M3TB6E - PUBLIC HEALTH IMPLICATIONS OF FEDERAL FUNDING PROVIDED FOR CERTAIN VIROLOGICAL RESEARCH

This tasker on EcoHealth is getting further bogged down. See below.

-----Original Message-----

**From:** (b)(6)  
(b)(6)  
**Sent:** Wednesday, January 5, 2022 1:29 PM  
**To:** (b)(6)  
(b)(6)  
**Subject:** RE: Tasker: CATMS19112021M3TB6E - PUBLIC HEALTH IMPLICATIONS OF FEDERAL FUNDING PROVIDED FOR CERTAIN VIROLOGICAL RESEARCH

(b)(6)

There are two separate taskers and I am waiting to hear from CB (why are we giving them information when we are giving information to NCB direct). I haven't heard back from A&S but I will ask the question.

(b)(6)

-----Original Message-----

From: (b)(6)

(b)(6)

Sent: Wednesday, January 5, 2022 1:27 PM

To: (b)(6)

(b)(6)

Cc: (b)(6)

(b)(6)

Subject: Tasker: CATMS19112021M3TB6E - PUBLIC HEALTH IMPLICATIONS OF FEDERAL FUNDING PROVIDED FOR CERTAIN VIROLOGICAL RESEARCH

(b)(6)

See below. Have you seen any traffic about this tasker getting extended by a few days?

Thanks,

(b)(6)

-----Original Message-----

From: (b)(6)

(b)(6)

Sent: Wednesday, January 5, 2022 10:15 AM

To: (b)(6)

Cc:

(b)(6)

Subject: PUBLIC HEALTH IMPLICATIONS OF FEDERAL FUNDING PROVIDED FOR CERTAIN VIROLOGICAL RESEARCH

H (b)(6)

Just a note that (b)(6) pushed base with (b)(6) office who issued this task, it will be extended to 11 Jan. It may not float down through CATMS yet, but if you could let the 4th floor know that'd be great.

Thanks

(b)(6)

-----Original Message-----

From: (b)(6)

(b)(6)

Sent: Wednesday, January 5, 2022 9:28 AM

To: (b)(6)

Subject: Tasker: CATMS19112021M3TB6E - PUBLIC HEALTH IMPLICATIONS OF FEDERAL FUNDING PROVIDED FOR CERTAIN VIROLOGICAL RESEARCH

BACKGROUND: The Senate Homeland Security Committee has asked for information related to DTRA's work with EcoHealth Alliance. They've requested: (1) All

research proposals or grant applications submitted by or on behalf of EcoHealth Alliance and/or the Wuhan Institute of Virology, and (2) All documents or communications sent by the agency in response to any research proposal or grant application submitted by or on behalf of EcoHealth and/or the WIV.

(b)(5)



SUSPENSE: 6 Jan 2021

**From:** (b)(6)  
**To:**  
**Subject:** RE: Tasker: EcoHealth Inquiry - CATMS19112021M3TB6E Public Health Implications of Federal Funding Provided for Certain Virological Research  
**Date:** Monday, January 3, 2022 11:33:00 AM

(b)(6)

Looks like the deadline already passed. Did they get an extension? Also, how did you receive the tasker? TMT?  
Hope all is well.

(b)(6)

Division Chief, Integration Management Division  
Defense Threat Reduction Agency (DTRA)

(b)(6)

-----Original Message-----

From: (b)(6)  
Sent: Monday, January 3, 2022 11:12 AM  
To: DTRA Ft Belvoir CT List CT DAG <dtra.belvoir.ct.list.ct-dag@mail.mil>; (b)(6)

(b)(6)

Subject: Tasker: EcoHealth Inquiry - CATMS19112021M3TB6E Public Health Implications of Federal Funding Provided for Certain Virological Research

CT & RD,

This morning, DTRA received an EcoHealth Alliance inquiry from the Senate Homeland Security Committee. The letter is dated 11/18/2021. (b)(5)

(b)(5) The questions they ask are as follows:

(1) All research proposals or grant applications submitted by or on behalf of EcoHealth Alliance (EcoHealth) and/or the Wuhan Institute of Virology (WIV).

(2) All documents or communications sent by the agency in response to any research proposal or grant application submitted by or on behalf of EcoHealth and/or the WIV.

(b)(5)

Thanks,

(b)(6)

(b)(6)

Legislative Liaison

Defense Threat Reduction Agency

(b)(6)

**From:** (b)(6)  
**To:**  
**Subject:** RE: Tasker: EcoHealth Inquiry - CATMS19112021M3TB6E Public Health Implications of Federal Funding Provided for Certain Virological Research  
**Date:** Monday, January 3, 2022 12:10:44 PM

Ma'am,

Yes, the deadline listed in the letter has passed, but apparently A&S requested an extension. The front office called me about this to let me know the item was coming down via TMT. I have since received it in TMT and tasked CT and RD to contribute.

Thanks,

(b)(6)

-----Original Message-----

**From:** (b)(6)  
**Sent:** Monday, January 3, 2022 11:34 AM  
**To:** (b)(6)  
**Subject:** RE: Tasker: EcoHealth Inquiry - CATMS19112021M3TB6E Public Health Implications of Federal Funding Provided for Certain Virological Research

(b)(6)

Looks like the deadline already passed. Did they get an extension? Also, how did you receive the tasker? TMT? Hope all is well.

(b)(6)

Division Chief, Integration Management Division Defense Threat Reduction Agency (DTRA)

(b)(6)

-----Original Message-----

**From:** (b)(6)  
**Sent:** Monday, January 3, 2022 11:12 AM  
**To:** DTRA Ft Belvoir CT List CT DAG <dtra.belvoir.ct.list.ct-dag@mail.mil> (b)(6)

(b)(6)

**Subject:** Tasker: EcoHealth Inquiry - CATMS19112021M3TB6E Public Health Implications of Federal Funding Provided for Certain Virological Research

CT & RD,

This morning, DTRA received an EcoHealth Alliance inquiry from the Senate Homeland Security Committee. The

letter is dated 11/18/2021, but R&E and A&S have been debating in the interim who is to respond and now a response is expected very soon. The questions they ask are as follows:

(1) All research proposals or grant applications submitted by or on behalf of EcoHealth Alliance (EcoHealth) and/or the Wuhan Institute of Virology (WIV).

(2) All documents or communications sent by the agency in response to any research proposal or grant application submitted by or on behalf of EcoHealth and/or the WIV.

(b)(5)

Thanks,

(b)(6)

Legislative Liaison

Defense Threat Reduction Agency

(b)(6)



**From:**  
**To:**  
**Subject:**  
**Date:**

(b)(6)

RE: Tasker: EcoHealth Inquiry - CATMS19112021M3TB6E Public Health Implications of Federal Funding Provided for Certain Virological Research  
Monday, January 3, 2022 12:22:35 PM

Looks like we will be on TW. Who in the front office usually contacts you? Just want to make sure I'm in the loop.

(b)(6)

Division Chief, Integration Management Division  
Defense Threat Reduction Agency (DTRA)

(b)(6)

-----Original Message-----

From: (b)(6)

Sent: Monday, January 3, 2022 12:11 PM

To: (b)(6)

Subject: RE: Tasker: EcoHealth Inquiry - CATMS19112021M3TB6E Public Health Implications of Federal Funding Provided for Certain Virological Research

Ma'am,

Yes, the deadline listed in the letter has passed, but apparently A&S requested an extension. The front office called me about this to let me know the item was coming down via TMT. I have since received it in TMT and tasked CT and RD to contribute.

Thanks

(b)(6)

-----Original Message-----

From: (b)(6)

Sent: Monday, January 3, 2022 11:54 AM

To: (b)(6)

Subject: RE: Tasker: EcoHealth Inquiry - CATMS19112021M3TB6E Public Health Implications of Federal Funding Provided for Certain Virological Research

(b)(6)

Looks like the deadline already passed. Did they get an extension? Also, how did you receive the tasker? TMT? Hope all is well.

(b)(6)

Division Chief, Integration Management Division Defense Threat Reduction Agency (DTRA)

(b)(6)

-----Original Message-----

From: (b)(6)

Sent: Monday, January 5, 2022 11:12 AM

To: DTRA Et Belvoir CT List CT DAG <dtra.belvoir.ct.list.ct-dag@mail.mil> (b)(6)

(b)(6)

Cc: (b)(6)

DTI

DTI

Subject: Tasker: EcoHealth Inquiry - CATMS19112021M3TB6E Public Health Implications of Federal Funding Provided for Certain Virological Research

CT & RD,

This morning, DTRA received an EcoHealth Alliance inquiry from the Senate Homeland Security Committee. The letter is dated 11/18/2021, but R&E and A&S have been debating in the interim who is to respond and now a response is expected very soon. The questions they ask are as follows:

(1) All research proposals or grant applications submitted by or on behalf of EcoHealth Alliance (EcoHealth) and/or the Wuhan Institute of Virology (WIV).

(2) All documents or communications sent by the agency in response to any research proposal or grant application submitted by or on behalf of EcoHealth and/or the WIV.

(b)(5)

Thanks,

(b)(6)

Legislative Liaison

Defense Threat Reduction Agency

(b)(6)

**From:** (b)(6)  
**To:**  
**Cc:**  
**Subject:** Review of EcoHealth activities  
**Date:** Wednesday, August 17, 2022 3:57:47 PM

---

(b)(6)

I wanted to follow-up on our EcoHealth discussion from yesterday.

(b)(5)

(b)(5)

Thanks!

(b)(6)

Legislative Liaison  
Defense Threat Reduction Agency

(b)(6)

Page 001 of 433

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 002 of 433

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act